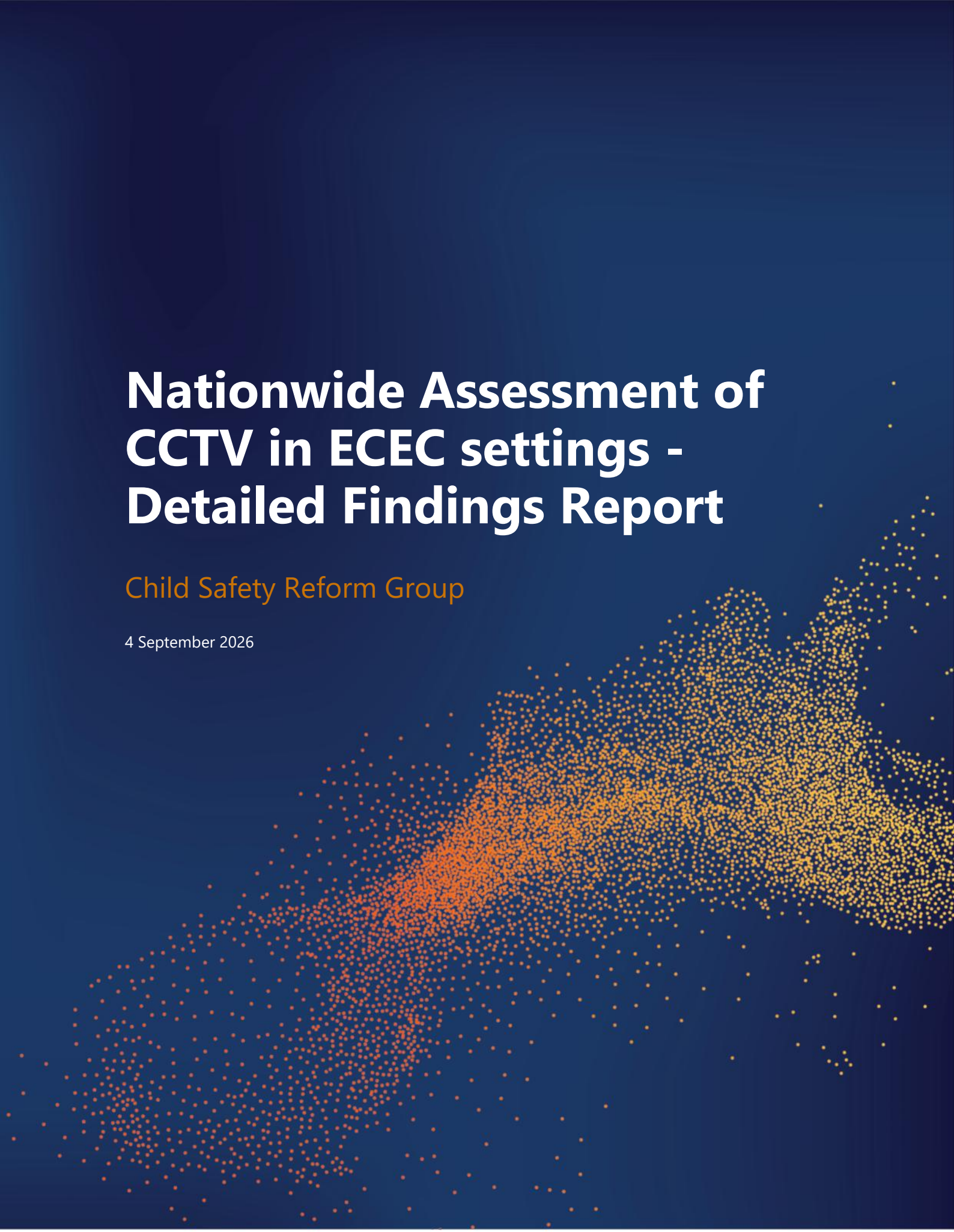
Nationwide Assessment of CCTV in ECEC settings - Detailed Findings Report

Child Safety Reform Group

4 September 2026



nous

Expert Panel



Contents

1 Background and context to the Assessment 1

1.1 Assessment design 1

1.2 Assessment implementation 5

1.3 Outcomes framework 14

2 Findings from the Assessment 16

2.1 Current state of CCTV in ECEC 16

2.1.1 Current state of CCTV adoption 16

2.1.2 CCTV uses in practice 24

2.2 Effectiveness of CCTV across child safety outcomes 31

2.2.1 Detection 31

2.2.2 Response 40

2.2.3 Prevention 44

2.2.4 Confidence in the use of CCTV 48

2.3 Costs of CCTV use 52

2.3.1 Installation costs 52

2.3.2 Operating costs for services and providers 58

2.3.3 Costs for regulatory authorities 59

3 Key findings and implications for future policy considerations 61

3.1 Conclusions 61

3.2 List of key findings 63

3.3 Future considerations for officials 67

3.4 Future considerations for the sector 67

Appendix A Outcomes framework 69

Appendix B Site visit case studies 74

Appendix C Additional CCTV market analysis 84

Appendix D Regulatory review 90

Appendix E Expert Panel 99

Appendix F List of participating providers 100

Appendix G Composition of Assessment participation 112

Glossary of key terms

TERM	DEFINITION
Aboriginal Community Controlled Organisations (ACCOs)	Services that build the strength and empowerment of Aboriginal and Torres Strait Islander communities and peoples and are: • incorporated under relevant legislation and not-for-profit • controlled and operated by Aboriginal and/or Torres Strait Islander peoples • connected to the community, or communities, in which they deliver the services • governed by a majority Aboriginal and/or Torres Strait Islander governing body.
Artificial Intelligence (AI)-enabled CCTV	CCTV systems that use artificial intelligence to automate functions such as risk detection, alerts, footage search or monitoring.
Assessment	The Nationwide Assessment of CCTV in Early Childhood Education and Care (ECEC) settings conducted between November 2025 and August 2026.
Camera blind spot	An area intentionally excluded from CCTV coverage due to privacy, legal or operational considerations.
Child Safety Reform Group (CSRG)	The interjurisdictional governance group established by governments to oversee implementation of the Assessment and provide strategic guidance on its design and delivery.
Closed-Circuit Television (CCTV)	A video surveillance system in which footage is transmitted within a closed network and access is restricted to authorised users.
Community of Practice (CoP)	A voluntary forum established during the Assessment's implementation phase that enabled participating services to share experiences and learn from peers.
Detection	The identification of issues, risks or incidents through CCTV footage, monitoring or review activities. This domain in the Assessment's Outcomes Framework considers the extent to which CCTV supports the timely and comprehensive identification of child safety issues, risks and incidents.
Early Childhood Education and Care (ECEC)	Provision of education and care that supports the holistic development of a child's social, emotional, cognitive and physical abilities in a way that meets each child's needs, building a solid and broad foundation for lifelong learning and wellbeing.
Incidents	A specific harmful or potentially harmful event that has occurred.4
Issues	A problem or concern identified through reports, observation or CCTV review that requires consideration in the context of ensuring a child-safe environment but falls short of a specific risk or actual incident.
Kindergarten/Preschool	Education and care provided for children in their year (or two years) before primary school, which meets specific requirements and is delivered by a teacher with a degree. Preschool education can be provided by standalone preschools/kindergartens or within long day care services.

TERM	DEFINITION
Long Day Care	A centre-based service providing all-day or part-time care for children aged birth to five years of age which may incorporate a kindergarten or preschool program.
Occasional care	An ECEC service that provides education and care for children on an occasional or flexible basis, typically for short periods and without requiring ongoing enrolment.
Outcomes Framework	Defines the outcomes the Assessment seeks to measure through associated indicators and data sources across four domains: detection, response, prevention and confidence.
Physical blind spot	An area that is not adequately captured by CCTV cameras due to coverage limitations or physical obstructions.
Prevention	The use of insights derived from CCTV footage to identify patterns, behaviours or circumstances that may reduce the likelihood of future harm occurring. This domain of the Assessment's Outcomes Framework considers how CCTV may contribute to continuous improvement and risk mitigation.
Privacy Impact Assessment	A systematic assessment of a project, initiative or major activity to identify potential privacy impacts that need to be managed, minimised or eliminated.
Proactive monitoring	The purposeful review or monitoring of CCTV footage to identify risks or issues before an incident occurs.
Provider	An approved provider responsible for the operation of one or more approved ECEC services. A provider may operate a single service or multiple services.
Reflective practice	The use of CCTV footage to support professional learning, service or quality improvement.
Regulatory Authority (RA)	The state or territory government authority responsible for regulating ECEC services.
Response	The use of CCTV footage to investigate, understand, verify and respond to issues, risks, complaints, allegations or incidents. This domain in the Assessment's Outcomes Framework considers the extent to which CCTV supports timely and effective responses to child safety concerns.
Retention Period	The length of time CCTV footage is retained by a CCTV system before being deleted, overwritten or otherwise disposed of in accordance with relevant governance requirements.
Risks	A potential source of harm that can or ought to be mitigated.
Scenario	A construct in the Assessment designed to explore different use cases for CCTV and identify any meaningful variations associated with different monitoring and review approaches.

TERM	DEFINITION
Service	An individual ECEC service or centre delivering education and care to children. For the purposes of the Assessment, eligible service types include long day care, kindergarten/preschool and outside school hours care services. Family day care services are excluded from the Assessment.
Service Usage Data	Data reported by Tier 2 participating services on CCTV operations, incidents, monitoring activities, system performance and collected throughout the Assessment.
Theory of Change	The framework developed for the Assessment that describes how CCTV is expected to contribute to child safety outcomes.
Tier 1 services	Services participating in the Assessment that provided baseline information but did not undertake Service Usage Data.
Tier 2 services	Services participating in the Assessment that contributed both baseline and ongoing evidence through Service Usage Data reporting and other Assessment activities.

1 Background and context to the Assessment

A series of high-profile child safety incidents in Early Childhood Education and Care (ECEC) services – including incidents of sexual abuse, neglect, and inappropriate disciplinary conduct – prompted governments to consider whether additional measures may be required to strengthen child safety arrangements. In response, Education Ministers agreed to undertake a nationwide assessment (the Assessment) of the use of Closed-Circuit Television (CCTV) in ECEC settings.

The Assessment was commissioned to build an evidence base on the use of CCTV in ECEC settings. It follows NSW's Independent Review of Early Childhood Education and Care Regulation (the Wheeler Review) and Victoria's Rapid Child Safety Review 2025, both of which identified CCTV as a potential tool to strengthen child safety and highlighted the need for further examination of its role within the sector. The work is informed by, and takes account of, the National Quality Framework (NQF) which ensures a national approach to regulation, assessment and quality improvement within the ECEC sector. In particular, consideration of the potential role of CCTV in strengthening child safety invokes Quality Area 2 of the National Quality Standard and the supervision requirements under the National Law, highlighting an important principle that underpins the Assessment: namely that CCTV should be seen as a complement to safeguarding arrangements, rather than a replacement for human supervision and good-quality education and care practices. Quality Area 7 of the NQF is relevant as well, given the role of service leaders in ensuring appropriate management of risk and the pursuit of opportunities to continuously improve quality of service delivery.

The Assessment examined the benefits, costs and risks associated with CCTV use, drawing on a variety of use cases that were explored through Assessment 'scenarios' (described in Figure 1 below). This final report distils the key findings, drawing on extensive research and analysis conducted between November 2025 and August 2026. Its purpose is to present evidence to inform policy decisions regarding the use of CCTV in ECEC services, including to better understand current practices and provide the basis for guidance on the safe, appropriate and effective use of CCTV in different ECEC settings.

The Assessment's design and implementation have been overseen by the Child Safety Reform Group (CSRG), and informed by engagement with all jurisdictions, key representative bodies, technical experts and the broader ECEC sector. Evidence has been drawn from more than 600 services that provided information through the initial Expression of Interest process, over 800 sector survey respondents and approximately 300 services, staff and families who actively participated in the Assessment.

The Assessment was delivered in two stages – a design phase and implementation phase – each of which is discussed in turn below.

1.1 Assessment design

The Assessment was designed from November 2025 to January 2026, drawing on desktop research, engagement with states and territories (including RAs), and larger multi-jurisdictional providers. Additionally, an Expert Panel was established that comprised: sector representatives, including Early Childhood Australia, National Aboriginal and Torres Strait Islander Education Corporation (NATSIEC) and relevant unions; government and non-government experts in privacy and surveillance; and ECEC experts, notably Professor Leah Bromfield, Director of the Australian Centre for Child Protection, as outlined in Appendix E.

Based on this research and engagement, the following reports were produced:

- **Environmental scan** – covering CCTV use in ECEC and comparable care settings in Australia, as well as current policy and practice in key overseas jurisdictions (including two where CCTV is mandatory in ECEC settings)

- **Literature Review** – exploring the available (limited) evidence on the extent to which CCTV may contribute to improved child safety through detection of unsafe practices or incidents of harm, as a deterrent, and as a tool to support investigations.
- **Theory of change** – which articulates the potential role of CCTV in relation to three types of harm: sexual abuse, physical harm (including unintentional 'heat of the moment' incidents), and neglect (e.g. not monitoring sleeping areas or perimeters appropriately). Importantly, the Theory of Change highlighted that CCTV was unlikely to have a deterrent effect on perpetrators of sexual harm. Nor would it be very useful in capturing incidents of such harm, given that they tend to occur in private areas in which CCTV cameras are prohibited.
- **Outcomes framework** – informed by the Theory of Change, this set out the higher-order key lines of enquiry for the Assessment (see section 1.3).

Nous also developed a plan for managing the legal, privacy, cybersecurity and ICT risks associated with the proposed Assessment.

Alongside ongoing engagement with CSRG, these documents informed the development of the Assessment design, which was subsequently formalised in the Assessment Framework and Parameters document. This document translated the Assessment's objectives into a clear and practical methodology, establishing the key research questions, scenarios to be tested, sample design, data collection arrangements, analytical approach, participation requirements and governance framework for the Assessment.

Six 'scenarios' enabled more targeted exploration through the Assessment.

To address those broad objectives, and specifically to determine the impact of CCTV on practice within ECEC services, the Assessment approach featured the use of six use case 'scenarios'. These broadly reflected variations across four dimensions, whether CCTV:

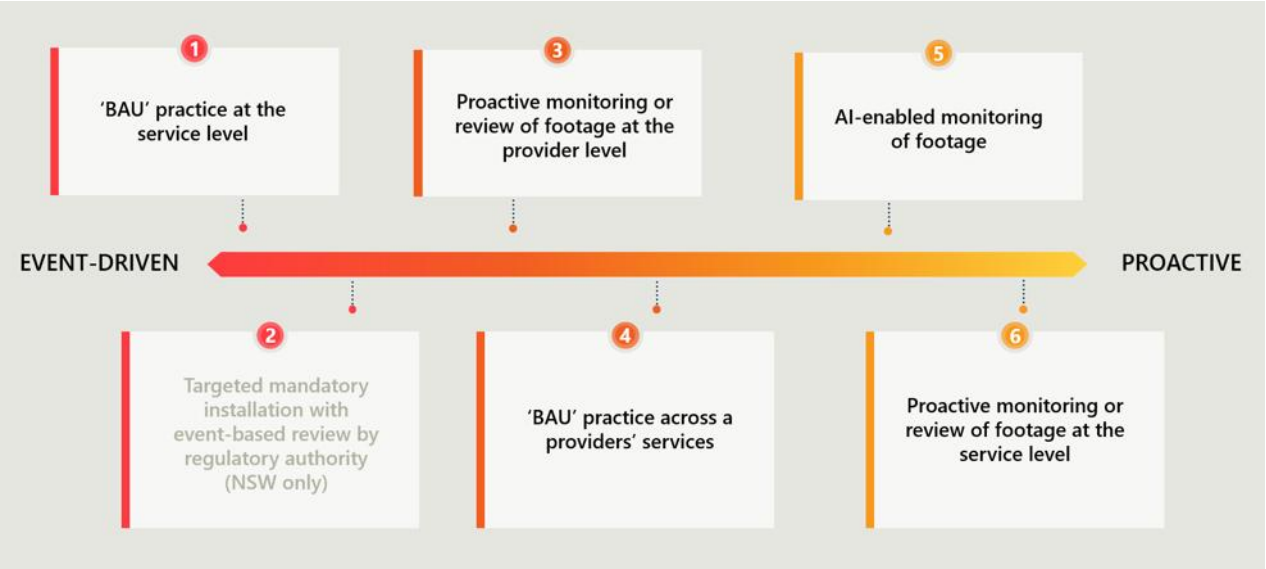
- Is used only in response to an identified or reported incident or also used 'proactively', which refers to either purposeful monitoring of live feeds or targeted retrospective review, using either a risk-based or random approach
- Was required by a regulatory authority or corporate headquarters, rather than being adopted at the service level by choice.
- Was monitored centrally (i.e. by corporate staff or the regulatory authority) rather than at the service level
- Systems had AI technology embedded that was being actively used.

The six scenarios are set out in Figure 1 overleaf.

As the Assessment progressed, practical implementation constraints meant some elements of the original design could not be fully tested, particularly mandatory participation models and central management of CCTV systems and footage by RAs (as discussed further below). While the scenarios evolved over time, the Assessment continued to generate evidence against the underlying assumptions and variables they were intended to explore.

It is important to note that, under all scenarios, RAs continued to access footage for investigative purposes in line with existing practice.

Figure 1 | CCTV Assessment Scenarios



The Scenarios are described in more detail below: As the Assessment progressed, practical implementation constraints meant some elements of the original design could not be fully tested, particularly mandatory participation models and central management of CCTV systems and footage by RAs (as discussed below). While the scenarios evolved over time, the Assessment continued to generate evidence against the underlying assumptions and variables they were intended to explore.

1. **Scenario 1 (81 services): 'BAU' practice at the service level** – This Scenario reflects current practices where CCTV installation is voluntary, and systems are managed at the service-level. It assumes that CCTV monitor feeds, if able to be viewed, are used incidentally, for ad hoc checks on who is present in one or more rooms, or to see what activities are underway. This Scenario therefore provides an understanding of current practices in ECEC services that have CCTV installed, including where cameras are typically placed, how footage is monitored and managed, and how current usage influences (or not) workforce behaviour and parent confidence about child safety.
2. **Scenario 2 (0 services): Targeted mandatory installation, with event-based review by regulatory authority** (NSW only) – In this Scenario, CCTV installation is mandated only for ECEC services identified as high-risk (e.g., with past safety issues or/compliance violations). Footage is intended to largely be accessed by the regulator to support investigations where concerns or allegations are raised. This Scenario aimed to assess the effect of targeted, mandated CCTV installation by the regulator. It did not proceed within the Assessment timeframes, however, due to legislative and operational complexities that delayed the implementation of NSW's proposed pilot. See the boxed text overleaf.
3. **Scenario 3 (5 services): Proactive monitoring or review of footage at the provider level** – In this Scenario, a provider's corporate safeguarding teams (separate from service-level operations), monitored or reviewed CCTV footage purposefully to explore whether there were issues or incidents not otherwise being detected by staff. They had the option to take a risk-based approach – e.g. focusing on high-risk areas or times of day – or randomly sampling footage. The aim of this Scenario was to explore the effects of provider-directed use of CCTV and 'arm's-length' monitoring or review.
4. **Scenario 4 (26 services): 'BAU' practice across a providers' services** – This Scenario covers situations where CCTV was installed at the direction of a provider across all their services, regardless of their risk profile. It assumed monitoring practices similar to Scenario 1 (i.e. where monitors are viewed for ad hoc checks as opposed to targeted monitoring or review). This Scenario explored the costs and operational impacts of using CCTV across multiple services, and whether a blanket approach would have a different effect on workforce culture compared to targeted, risk-based installation.

5. **Scenario 5 (5 services): AI-enabled monitoring of footage** – This Scenario was to explore the potential for AI to enable something closer to continuous monitoring. Where AI functionality is available, the system is programmed and calibrated to identify risks or unsafe behaviours, and to issue real-time alerts. Staff manually review footage based on the alerts, including to check for 'false positives'. The Scenario aimed to assess the feasibility, costs, value and risks of using AI in this way, noting that it is an emerging technology.
6. **Scenario 6 (43 services): Proactive monitoring or review of footage at the service level** – In this Scenario, services commit to regular 'live' monitoring of footage (e.g. during peak times) or targeted retrospective review (i.e. on a risk- or random sampling basis), as for Scenario 3. This Scenario sought to gauge whether regular self-review strengthens safety culture and improves practices, while also examining staff resource requirements and feasibility of implementation.

It is important to note that, under all scenarios, RAs continued to access footage for investigative purposes in line with existing practice.

The design of NSW's targeted mandatory CCTV trial highlighted key legislative, governance and operational considerations for regulator-managed CCTV models.



NSW's trial, reflected in the Assessment's Scenario 2, has been designed to test a targeted mandatory CCTV model for higher-risk services. The NSW Government committed to this model in response to recommendations of the Wheeler Review. The trial was intended to test the mandatory use of CCTV among a small number of services based on a risk analysis.

By concentrating investment and regulatory effort on services with elevated risk profiles, the model seeks to examine whether CCTV could strengthen safeguarding and regulatory oversight in higher-risk settings without the costs associated with broader implementation. The trial is also intended to test whether regulator-managed CCTV could strengthen accountability and provider compliance, while providing an objective source of evidence to support the investigation of any concerns.

Under the model, CCTV is to be installed in services identified through regulatory risk indicators (e.g. prior prosecutions, suspensions or confirmed breaches), with installation and operating costs funded by government. Unlike other Assessment scenarios, footage is to be stored and managed centrally by the NSW Early Learning Commission. Footage is intended to largely be accessed by the regulator to support investigations where concerns or allegations are raised.

Legislative and operational complexities associated with the design of this model have resulted in a longer implementation lead time than originally anticipated, and commencement timing has not yet been confirmed.

While operational findings for the trial are not available for inclusion in the Assessment, the design and preparatory processes for the NSW trial offer useful insights relevant to regulator-managed CCTV models, particularly in relation to legislative enablers and barriers, and technology options.

Further insights are expected from NSW's implementation, particularly with regard to the:

- Operational demands placed on regulators when footage is stored and managed centrally,
- Design of access controls, permissions and notification arrangements for participating services,
- Management of footage access requests and associated evidentiary requirements,
- Approaches to procuring and deploying CCTV systems across multiple sites, including opportunities to leverage centralised purchasing and installation arrangements,
- Effectiveness and efficiency of targeting CCTV deployment to services identified as higher risk,
- Extent to which regulator-managed CCTV supports the verification of concerns, provider accountability and deterrence in higher-risk settings.

1.2 Assessment implementation

The implementation phase of the Assessment was undertaken between January and July 2026. During this time, the Assessment team recruited and onboarded participating services, established a nationally diverse sample and supported services to participate in the Assessment.

The following sections describe the Assessment's approach to service recruitment and sampling and the broader features of the implementation phase.

Service recruitment and sampling

A total of 643 services expressed interest in participating in the Assessment, of which 309 ultimately took part. They divided into two tiers of participation (described below). They were initially informed of the Assessment through a webinar held on 19 December 2025, which preceded a process calling for Expressions of Interest (EoI). The EoI process was conducted in two stages:

- **Stage 1** (22 December 2025 to 23 January 2026) – collected information required to support development of an appropriate national sample, including information on service type, location, ownership structure, existing or planned CCTV infrastructure, and Assessment Scenario preferences.
- **Stage 2** (from 12 January 2026) – sought more detail from those services deemed eligible to proceed, including on their CCTV, data governance, privacy and cybersecurity policies. Services also confirmed completion of a Privacy Impact Assessment (PIA) and provided information on consent protocols, data retention settings and footage access arrangements.

Shortlisted services were reviewed by jurisdictions to confirm agreement to their participation.

Two-tier model of participation

Information collected through the EoI process enabled Nous to assess service eligibility and develop a participant cohort that balanced national representation with the Assessment's data collection requirements. Participating services were then grouped into two tiers of involvement according to their level of participation: those which had contributed detailed baseline information and that might be willing to provide additional, targeted inputs; and those that would provide fortnightly reports during the Assessment. This enabled the Assessment to capture both a broad picture of CCTV uses across the sample, and more granular evidence on how CCTV was being used in practice. The division of the 309 total participating services into two tiers is as follows:

- **Tier 1 (baseline evidence)** comprised 309 services from the nearly 15,500 family day care, long day care, outside school hours care and preschool/kindergarten services operated by approved providers across Australia.[1] 149 of these services completed the Stage 2 eligibility assessments but did not ultimately participate in ongoing reporting on CCTV use in practice. These services provided information on service characteristics, CCTV infrastructure, governance arrangements, privacy settings and attitudes towards CCTV. This established a baseline picture of CCTV use across participating services and those that withdrew or did not meet the eligibility criteria to progress, with the challenges of some of these services discussed throughout section 2.1.
- **Tier 2 (active reporting)** comprised 160 services that participated in ongoing reporting on CCTV use in practice, providing data on incidents where CCTV was used to review what happened or to support investigations by the regulatory authority, and issues with CCTV equipment. Services participating in proactive monitoring scenarios also reported their observations relevant to the management of child safety risks, and services using AI-enabled technologies advised on system alerts and the proportion of 'false positives'.

[1] ACECQA, NQF Annual Performance Report, December 2025 (accessed 19 August 2026), https://www.acecqa.gov.au/sites/default/files/2025-12/2025-NQF-Annual-Performance-Report.pdf

Eligible Tier 2 participating services received Australian Government payments commensurate with their level of engagement with the Assessment, recognising the time and effort required to meet reporting requirements. A small number of Tier 1 services also received payments in recognition of their contribution to additional evidence-gathering activities, including surveys and site visits.

Sampling approach

The sampling approach was designed to achieve geographic and operational diversity across participating services. Jurisdictional targets were established in proportion to the national distribution of approved services. The Assessment sought national representation across the following:

- Geographic location (metropolitan, regional, rural and remote)
- Service type (long day care, preschool/kindergarten, and outside school hours care)
- Ownership structure (community-based, private, and local government or not-for-profit)
- Provider size (small, medium and large).

The Assessment also sought to include Aboriginal Community Controlled Organisations (ACCOs) and other services that reported a high proportion of First Nations children. While two ACCOs participated in Tier 1, no ongoing operational data was provided through Tier 2 participation. This is discussed further below.

Note that neither Family Day Care nor in-home care services were included in the scope of the Assessment. The Evaluation of the Assessment will, however, consider these models of ECEC and the extent to which CCTV may play a role in supporting child safety in those contexts.

Overall, the final participant cohort included services from all jurisdictions and broadly reflected diversity across geographic locations, service type, ownership structure and provider size.

Jurisdictional representation

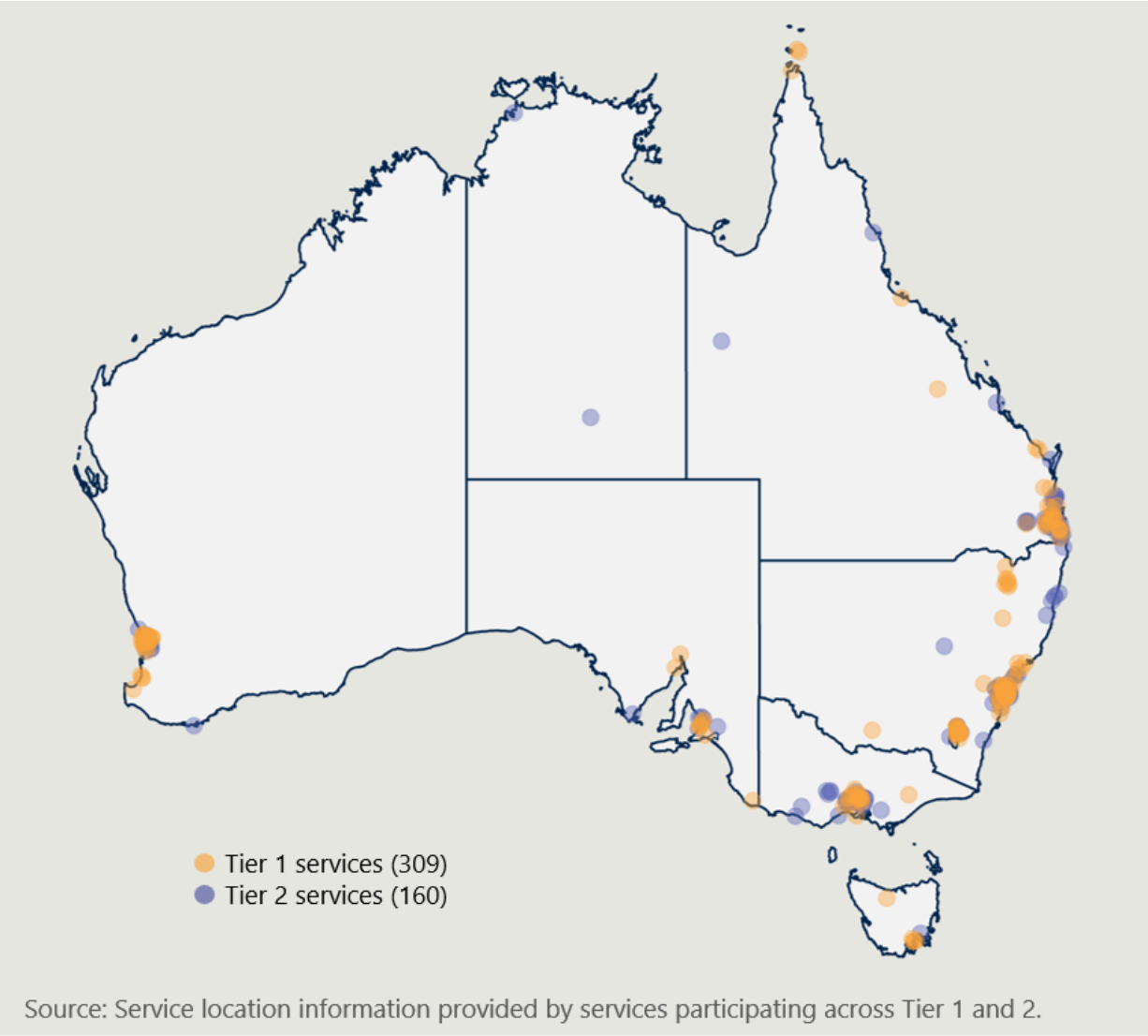
Table 1 compares jurisdictional recruitment targets with the final sample.

Table 1 | Sample targets and final composition, by jurisdiction

Jurisdiction	Target sample (n)	Final Tier 1 sample (n)	Final Tier 2 sample (n)
NSW	115	92	44
VIC	65	53	36
QLD	62	77	50
WA	27	42	14
SA	17	16	7
ACT	6	21	6
TAS	5	6	1
NT	3	2	2
Total	**300**	**309**	**160**

The geographical distribution of the services is mapped in Figure 2 overleaf.

Figure 2 | Location of participating services by tier



Source: Service location information provided by services participating across Tier 1 and 2.

Variations in the representativeness of service types

While broadly representative of the different service types and ownership structures in the ECEC sector, some important differences should be considered when interpreting the findings of the Assessment:

- **Over-represented in the Assessment** were Long Day Care services, private for-profit services and small-to-medium providers.
- **Under-represented in the Assessment** were Outside School Hours Care (OSHC), Preschool/Kindergarten services and large providers.

As a result, the Assessment findings are likely to be most reflective of Long Day Care settings and the experiences of private and smaller providers. Please see a detailed summary of the representativeness of services participating in the Assessment in Appendix G.

The Assessment pursued a range of strategies to improve the representativeness of the sample. These included:

- Active follow-up and repeated engagement with services to assist in removing any barriers to participation.
- Work with States and Territories to identify government preschools to potentially include.

- Flexibility to join the Assessment part-way through to allow for privacy and other policies to be completed, or for CCTV to be installed as per the operators' intentions as reporting during the Expression of Interest process.

Importantly, there were no material variations in the majority of findings by jurisdiction, level of remoteness, service type, ownership type or provider size. Exceptions to this are noted in the relevant sections of the report.

Participation by Aboriginal Community Controlled Organisations (ACCOs)

The Assessment made special efforts to recruit and onboard ACCOs, recognising that there may be specific cultural considerations associated with the use of CCTV in some First Nations communities, including communities where historical experiences of surveillance and government intervention remain important considerations.

Nous engaged with NATSIEC and SNAICC (through targeted discussions before and after the Assessment's implementation) on these matters, reaffirming that the intent of the Assessment was not to promote the use of CCTV but to explore how it was already being used in ECEC settings, with a view to understanding both the risks and the benefits. This engagement also sought to test interest in participation by First Nations services and identify any considerations relevant to their involvement in the Assessment. At the same time, the Australian Department of Education ensured that special provision was made in its Participation Payments grant scheme to compensate ACCOs specifically (as well as smaller and more remote services generally) for being part of the Tier 2 data collection process.

Two First Nations services participated as Tier 1 Assessment participants and were initially expected to continue into Tier 2 participation. However, due to operational constraints during the Assessment period, neither service was ultimately able to commit to the Tier 2 data collection process.

Aware of the risks of under-representation of this important provider type, and of the First Nations perspective on CCTV more generally, the Department asked that the Evaluation focus on engaging with SNAICC and NATSIEC to explore more deeply the particular cultural considerations and associations with CCTV which must be carefully considered in any relevant policy making and good practice guidance.

Representation based on CCTV configurations

All participating services either had CCTV in place before the Assessment began or installed it as a condition of participation. Some had external cameras only, or only a few interior and exterior cameras, while others had more sophisticated systems (see Case studies 1 and 2 in Appendix B). Some sites had cameras installed for property security reasons, providing secondary value in terms of child safety benefits, while others had CCTV installed with the primary intent to improve child safety). It is unclear how representative these features are across the entire ECEC sector. Additionally, it cannot be gauged the extent to which systems installed for one purpose came to be used for broader purposes and over what timeframe. However, participants noted a strong child safety dimension to their use of CCTV, which has been reflected in the findings of the Assessment.

Representation based on risk profiling

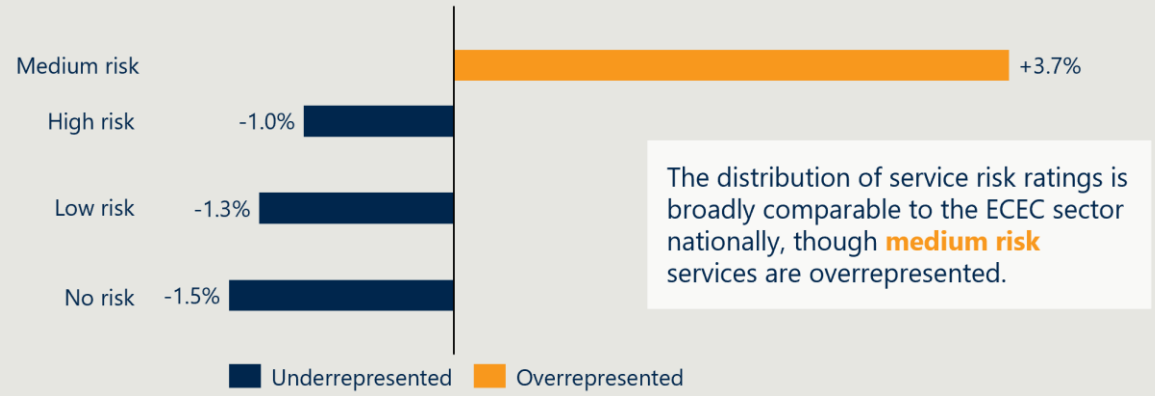
According to independent analysis by the Department using National Quality Agenda IT System (NQA ITS) data[2], participating services have a similar distribution of high, medium, low and no risk ratings to the sector as a whole. This suggests that the sample is not skewed towards either lower- or higher-risk services.

As indicated in Figure 3, the distribution of service risk ratings across the four NQA ITS risk categories (high, medium, low and no risk) were broadly comparable to the ECEC sector nationally, with no statistically significant differences and only negligible effect sizes. The only notable variation was a slightly higher

[2] Disaggregated analysis of participating services and the national ECEC sector provided by the Australian Government Department of Education using data from the National Quality Agenda IT System (NQA ITS).

proportion of medium-risk services among participating services (14.7 per cent compared with 11.0 per cent nationally), although this difference was modest in practical terms.

Figure 3 | Representation of service risk ratings in the Assessment sample



Source: Disaggregated analysis of participating services and the national ECEC sector provided by the Australian Government Department of Education using data from the National Quality Agenda IT System (NQA ITS)

It is important to note that the NQA ITS risk framework is intentionally weighted towards more severe quality and safety concerns, including prosecutions. While appropriate for identifying services with elevated overall risk, these higher-weighted indicators are not necessarily those most relevant to the CCTV Assessment, which is also concerned with lower-severity incidents and concerns that occur more frequently in ECEC settings.

To assess whether the similarity in overall risk ratings masked differences in these more relevant indicators, the Department analysed the four individual risk factors underpinning the NQA ITS framework. Participating services were broadly comparable to the national population across three of the four measures. Rates of incidents confirmed breaches and statutory compliance actions did not differ significantly from the broader sector, with all differences exhibiting negligible effect sizes. Complaints resulting in compliance action were the only measure to differ materially, with participating services recording a higher prevalence than the national population (9.8 per cent compared with 4.5 per cent).

Taken together, these findings provide confidence that participating services were representative of the broader ECEC sector on the incident, compliance and reporting-related indicators most relevant to the Assessment. While the sample was not perfectly representative across all service characteristics, both the overall risk ratings and underlying risk indicators suggest it provides a reasonable basis for interpreting the Assessment findings.

Data collection methods.

The Assessment drew on a broad range of quantitative and qualitative evidence collected throughout implementation. Evidence was collected from participating services, providers, staff, parents and caregivers, RAs and other stakeholders to understand how CCTV was implemented and its uses.

Importantly, the Assessment did not include direct engagement with children. This was for practical constraints, including the lack of time to complete an ethics approval process, and the challenges of communicating with pre-verbal or non-verbal children. There was also the risk of sensitising children to the cameras in a way that might have had unintended consequences.

Figure 4 | Overview of data collection methods



Service usage data

Tier 2 services completed service usage data each fortnight, tailored to their respective scenarios. All participating services reported incidents occurring within their service, including whether CCTV footage was available, reviewed, or used to support understanding of the incident.

Information was collected using a standard template provided to services that covered: date of incident, time of incident, date the incident was raised, type of harm, location of incident, how the service became aware of the incident, primary action taken, level of available CCTV footage, and reasons for partial or no footage.

Services undertaking proactive monitoring or review under their assigned Scenario provided additional information, customised to their participation, covering: date of review, whether the service monitored or reviewed CCTV content, time of day, date of CCTV footage, whether footage was risk-based or randomly selected, duration of review, camera location, any issues with footage access, whether footage identified anything, and how any issues related to types of harm.

Services using AI-enabled technology under Scenario 5 completed a separate form in addition to incident reporting, to examine the accuracy of AI use and the number of alerts in each reporting period. While services were asked to report on a common set of metrics (including total system downtime during service operating hours, where relevant; total alerts generated; false positives; and false negatives), they were permitted to customise their reporting to better reflect the capabilities, outputs, and performance of their AI-enabled systems.

The service usage data recorded whether an incident was reported to RAs, and whether it was available and used for an investigation outcome. It also documented information about CCTV operational outages or technical issues, and any changes to settings or access.

Surveys

Surveys were administered across multiple stakeholder groups, including services across the broader ECEC sector, participating Tier 1 and 2 providers, service and centre managers, staff, and parents and caregivers to capture perceptions of CCTV and their perceived benefits or disbenefits in ECEC settings.

Prior to the commencement of the Assessment, a sector-wide 'Provider Survey' was administered to providers across the ECEC sector. This survey received 861 responses and established baseline evidence on current state use of CCTV in ECEC and reasons for its implementation.

For participating Tier 2 services, surveys were administered in two waves: at the commencement of participation and towards the end of the Assessment. This enabled changes in experiences and perceptions of CCTV to be examined over time. Surveys were completed by provider head office representatives, service and centre managers, and staff. To support comparison with the broader sector, a select group of Tier 1 services completed the CCTV Experience Survey. This survey incorporated key questions from Service/Centre Manager Surveys 1 and 2 to capture experiences of CCTV implementation and use in services that were not participating in the Assessment.

A separate parent and caregiver survey was distributed through participating Tier 2 services to capture parent and caregiver perspectives on CCTV use in ECEC settings.

Table 2 provides an overview of surveys administered and response numbers.

Table 2 | Surveys administered through the Assessment

Survey	Purpose	Responses
Sector-wide Survey	Designed for services across the ECEC sector, this survey established baseline evidence on current CCTV use, service characteristics, reasons for using or not using CCTV, and key operational, privacy and workforce considerations.	861 responses

First wave	**Head Office Survey**	Established why providers were implementing CCTV, their governance arrangements, expected benefits and risks, and their planned approach to the Assessment.	10 responses
	Service / Centre Manager Survey 1	Designed for those who manage participating services, this survey established baseline evidence on service-level CCTV practices, including implementation approaches, day-to-day use, and impacts on service operations.	155 responses
	Staff Survey 1	Established baseline staff views on CCTV, covering child safety, educator practice, workplace culture and approaches to incidents	760 responses
Second wave	**Service / Centre Manager Survey 2**	Examined how CCTV was implemented and used in practice, including service-level impacts, implementation challenges and lessons learned.	104 responses
	Staff Survey 2	Explored workforce experiences of CCTV use in practice, including impacts on educator practice, workplace culture, perceptions of child safety and service operations.	482 responses
	Withdrawn Services Survey	As the only survey completed by Tier 1 service/centre managers, this survey examined CCTV implementation and use in practice, including operational impacts, implementation challenges, and lessons learned.	8 responses
	Parent and Caregiver Survey	Parents and caregivers at participating services were asked on their perspective on CCTV use in ECEC settings, including perceived benefits, concerns and impacts on confidence in service safety.	365 responses

Communities of Practice sessions

Fourteen Communities of Practice (CoP) sessions were conducted for Tier 2 participating services to support engagement in the Assessment and generate insights on how services configured, governed and used CCTV in practice. They were voluntary and held every 2-3 weeks. The Assessment recorded 238 attendances across all CoP sessions, with each session (conducted online) running for an average of 45 minutes each.

The CoPs were structured to cover the following themes:

- **Getting started in the Assessment** – overview of the Assessment, onboarding experiences and early preparation experiences for participation.
- **Early participation experiences** – services' initial reflections on participation, including staff and families' responses to participation and reporting experiences.
- **AI-enabled monitoring** – an opportunity for the five services participating in Scenario 5 to share reflections.
- **Child safety, harms, risks and CCTV** – services' accounts of how CCTV has assisted in identifying, understanding and responding to child safety incidents and risks.

- **Workforce and culture effects** – impacts of CCTV on workplace culture, staff wellbeing and professional relationships.
- **Costs, choices, and management practices** – services' decision-making process and approaches to managing CCTV systems, determining the appropriate CCTV system for their service and the costs associated with having it.
- **Assessment reflections and lessons learned** – participant reflections on the Assessment process, perceived benefits and drawbacks of CCTV, lessons learned through participation. This included lengthy discussions on proactive monitoring and reflective practice.

This structure allowed the Assessment to capture perspectives from services as their participation evolved, and to understand how experiences, challenges and perceived outcomes changed over time.

The conversations in the CoP sessions complemented regular ad hoc conversations that the Assessment implementation team had with individual services through its helpdesk. On average, the Assessment coordination team fielded four calls a day over a 4-month period.

Site visits

Sixteen site visits were undertaken of ten in-person visits and six virtual (i.e. online only) visits, including two with Tier 1 services. Site visits were conducted to understand how CCTV was implemented and used in practice. Services were purposively selected to provide coverage across Assessment scenarios, jurisdictions, service types and provider sizes.

Insights from the site visits informed the Assessment's findings and are the subjects of the case studies in Appendix B.

Regulatory authority engagements and data requests

Nous engaged with RAs in all eight jurisdictions, as well as ACECQA, through interviews and consultations. Data requests were issued to the eight state and territory RAs. This work examined the extent to which and how CCTV footage is used in regulatory investigations and broader sector oversight, and the barriers to access (e.g. short data retention periods) as well as the resource implications associated with its use, and regulators' views on the benefits and drawbacks of CCTV as a tool to support child safety.

Data limitations and caveats

The Assessment findings are informed by a broad and diverse evidence base. Nevertheless, several considerations should be kept in mind when interpreting the findings and recommendations:

- **The Assessment data collection period was relatively short, and so it is not possible to draw definitive conclusions about long-term child safety outcomes.** The Assessment was designed to generate evidence within agreed reporting timeframes and primarily involved services that already had CCTV systems in place, reflecting both implementation constraints and the Assessment's focus on understanding CCTV use in practice. Tier 2 reporting occurred over a 4-month period, and for many participating services, CCTV use was already established rather than newly introduced. While the Assessment cannot determine whether CCTV improves child safety outcomes or establish a causal relationship between CCTV use and child safety, it does provide evidence on how CCTV is used in practice and the circumstances under which it may support child safety, incident management and related operational outcomes.
- **The Assessment was not randomly selected, as participation was voluntary and subject to eligibility requirements.** Assessment findings reflect the experience and perspectives of services already using CCTV to some degree – some where it had been installed for a longer period of time, and others where it was added more recently. The sample of Assessment participants did not include a comparison group of services without CCTV, although some survey data was initially collected from those without CCTV.

- **Scenario 2 could not be tested as initially designed.** Legislative and operational complexities prevented implementation of the NSW targeted mandatory CCTV trial within the Assessment timeframes. As a result, the Assessment cannot draw on operational findings, but has been able to consider lessons arising from the design and development of the model, including legislative and technology considerations.
- **Much of the evidence base relied on self-reported and qualitative data.** The Assessment drew heavily on service surveys, service usage data, Communities of Practice and stakeholder consultations. While some quantitative data was available, including limited data from RAs and information provided by services on matters such as CCTV costs, much of the evidence reflects participant perspectives and experiences and could not be independently verified. This limitation was mitigated by the size of the participant cohort and the use of multiple evidence sources, which enabled findings to be tested across different datasets and perspectives.
- **Response rates to surveys varied, potentially affecting representativeness.** Although all surveys achieved responses from a majority of participating services, completion rates differed across survey rounds and cohorts (see Table 2). This means that some findings are based on a broader evidence base than others, and may not fully capture the views and experiences of all participants. Survey findings should therefore be considered alongside other Assessment evidence, including service usage data, Communities of Practice and stakeholder consultations.

The Assessment was designed to draw on multiple, independent sources, fortnightly service usage data, surveys, site visits, Communities of Practice and direct engagement with regulators, so that findings rest on more than any single method or perspective. Where these sources point consistently in the same direction, the findings can be held with confidence. Where the evidence is thinner or drawn from less well-represented groups, this is noted in the relevant sections.

Another point to consider in interpreting the Assessment findings, relating to the effect of the Assessment itself on behaviour by participating services (especially Tier 2 services), is the influence of the Assessment on how services think about and use their CCTV systems. Participation prompted services to review and reconsider how they had implemented CCTV and how they were using it. For example, a system may have been installed for some time, and while early consideration may have been given to careful camera placement and maintenance of appropriate privacy and data policies, attention to such details may diminish over time unless there is a trigger to re-visit these aspects of CCTV use.

Services indicated that the process of onboarding services into the Assessment incentivised many to complete or update their policies, or to consider anew how they were configuring their CCTV systems. Similarly, engagement with services in Communities of Practice and similar consultations led to open exchanges of information and discussions about different practices. They therefore had a modest capability-building effect.

While this does not appear to materially affect the findings, it suggests the Assessment was not entirely a 'natural experiment', despite efforts to minimise disruption to existing practice through the inclusion of 'business-as-usual' scenarios.

1.3 Outcomes framework

The outcomes framework guided the Assessment design, research activities and analysis to ensure comprehensive and well-evidenced findings. Key Lines of Enquiry were drawn from indicators related to five outcome domains: detection, response, prevention, confidence in the sector's use of CCTV and evidence to inform policy making. Examples of indicators included changes in staff behaviour, improvements in incident investigation and resolution, and reported in parental attitudes towards CCTV.

As noted above, given the Assessment's duration, as well as the range of factors influencing child safety outcomes, changes in rates of harm could not be reliably measured or attributed to CCTV use. Leading

indicators such as those cited above therefore provided a practical basis for assessing whether conditions associated with improved child safety were moving in the intended direction.

A full list of outcomes and indicators is provided in Appendix A.

2 Findings from the Assessment

2.1 Current state of CCTV in ECEC

This section examines the current state of CCTV in the ECEC sector. It outlines the extent of CCTV adoption, the factors influencing installation decisions and the role of regulatory requirements, and the characteristics of CCTV systems currently operating in ECEC settings.

2.1.1 Current state of CCTV adoption

Child safety concerns are fuelling demand for CCTV.

Survey findings suggest that approximately 23-30 per cent of services have CCTV installed.[3] This is broadly consistent with evidence from the Wheeler Review, which also identified CCTV as an established practice in a proportion of ECEC services.[4] Where CCTV is in place, coverage typically focuses on entrances, exits, perimeters and other external areas rather than providing comprehensive coverage across services. Existing CCTV systems were often installed for reasons of property security rather than child safety. However, use of CCTV for broader purposes appears to be increasing. Several large providers have implemented, or are implementing, CCTV across their service networks. This is largely driven by increasing interest in strengthening child safety measures.

The market is responding to this demand: some services reported an increase in outreaches from CCTV installers in anticipation of this heightened interest. A major CCTV installer noted that demand for CCTV in the ECEC sector is "going ballistic," driven by increased public scrutiny and media reporting on child sexual abuse.[5] It appears that the market for CCTV installers is growing quickly in response – 19 per cent of members of the peak body for Australia's security industry providing CCTV services were established in the last six years.[6]

Changing family expectations are also emerging as a driver of adoption. Survey findings suggest that around half of the service leaders who responded primarily valued CCTV for its role in supporting investigations, while around one quarter felt that the key benefit of CCTV was its ability to help families feel confident in the service's ability to ensure child safety.[7] These views were reflected in the Parent and Caregiver Survey, where 86 per cent of respondents agreed that CCTV increases their trust in the service's capacity to keep children safe.[8]

Operational, financial and organisational considerations drive CCTV installation decisions.

The Assessment was carefully designed to avoid creating an incentive for services to install CCTV where this was not already part of their plans. Participation payments were not to be used for the purchase or installation of CCTV, and only services that already had CCTV operational were eligible to participate. That said, the Assessment did have the effect, in some cases, of bringing forward plans for installation. Of interest is that some Assessment participants installed CCTV because they thought it inevitable that all services would eventually be expected to have it.

---

[3] According to Nous' whole of sector survey, CCTV use was at 30.3%, consistent with the Wheeler Review estimates for the sector in NSW (30%). A KPMG survey of the sector for the evaluation that accompanies this Assessment found that 23.5% of respondents used CCTV, excluding services who participated in the Assessment.

[4] Chris Wheeler Consulting, Independent review into the NSW Early Childhood Education and Care Regulatory Authority, May 2025 Final Report - Early Childhood Education and Care Regulation in NSW Independent Review - May 2025

[5] Consultation with CCTV installer

[6] Derived from a review of Australian Business Register data of Australian Security Industry Associate Limited (ASIAL) members identified as providing CCTV sales and installation services, as of July 2026. The establishment date of a business was defined as its ABN commencement date.

[7] Service / Centre Manager Survey 2

[8] Parent and Caregiver Survey.

Participating services identified a range of motivations for adopting CCTV. These included responding to heightened family expectations following media attention on the sector, supporting broader child safety strategies, and enhancing services' ability to investigate incidents and respond to allegations or complaints.[9]

Services reported several perceived benefits associated with CCTV adoption:

- Reinforcing professional accountability by creating an objective record that can help identify inappropriate behaviour. Several providers described CCTV providing a "black and white" account of events that helps determine whether something happened or not.[10]
- Deterring harmful behaviour by having CCTV in areas that cover staff interactions with children. Providers reported that CCTV strengthened oversight in classrooms and outdoor environments, with one provider noting that it had made "a huge difference" following incidents that previously could not be independently verified.[11]
- Providing reassurance to families by providing a resource to support claims and concerns raised by families. As one provider noted, CCTV gives families "a lot more confidence in our honesty" because services can provide evidence that reported events occurred as described.[12]
- Insurance considerations were identified as an additional benefit for a few services. A limited number of participating services described CCTV as improving insurance outcomes and lowering premiums by enhancing site security, particularly through monitoring external areas and reducing risks associated with theft, vandalism and unauthorised access.[13]

Most older CCTV systems were installed for property security and then upgraded over time.

Of the 309 services participating in the Assessment, the majority had CCTV systems that had been installed before child safety became a prominent issue in the media. As noted above, these systems were often initially introduced to deter and respond to theft and vandalism, and camera placement reflected this. As such, they were more likely to be external cameras only.

It is important to note in this context that, notwithstanding this limitation, outside cameras were nevertheless seen as providing important child safety benefits. Most obviously, they were valuable in recording playground accidents and interactions, which comprised a significant proportion of incidents reported. For example, almost 53% of incidents recorded in Service Usage Reports occurred outdoors. Reviewing footage from external areas not only revealed what circumstances led to an incident, but also exposed ongoing risks and areas requiring closer supervision by staff.

There were a range of what might be termed as secondary child safety benefits from external cameras as well. Multiple services operating in areas with observable levels of crime described external cameras as helping to reduce risks to children, families and staff by discouraging activity that could expose them to hazards such as discarded drug paraphernalia.[14] Participants also noted that external cameras helped to monitor access, potentially deterring individuals with malicious intent.[15] Some services further observed that the presence of cameras encouraged safer behaviour by parents and carers in pick-up and drop-off areas, including greater use of seatbelts and reduced incidents of leaving children unattended in vehicles.[16]

In many cases, services that originally had external cameras only expanded coverage or otherwise adapted these systems over time to be more useful from a child safety perspective. In addition to increasing the

[9] CoPs
[10] Ibid
[11] Site visit
[12] Ibid
[13] CoPs
[14] Site visits
[15] Site visits
[16] Ibid

number of cameras, services described replacing ageing equipment, introducing new functionality or integrating additional components with existing infrastructure.

In CoP discussions, it emerged that upgrade pathways are not always straightforward, however, with some services reporting uncertainty about how older systems could be expanded or integrated with newer technologies. Upgrade decisions were often informed by advice from installers or vendors, particularly to overcome technical constraints or compatibility issues. The point was made that such upgrades could be costly: one service, for example, reported investing approximately $7,000 over an 18-month period to address faults and modernise its CCTV system.[17]

Specialist CCTV installers are often, but not always, used.

Services reported using a range of approaches to procure, install and manage CCTV systems. It was common for providers to have engaged specialist installers, electricians, security providers, technology vendors or IT personnel to support system selection, installation and maintenance. Others described more informal approaches, including drawing on parents, family members or friends with technical expertise.[18] These different approaches contributed to the variation in how much CCTV systems cost to install and maintain, and in how they were configured.

Specialist expertise often continues to play a role after installation. Several participants said they relied on installers or technology providers to advise on system functionality, camera placement, storage arrangements and future upgrade options.[19] During the process of being onboarded into the Assessment, some services required assistance from installers, security providers or IT personnel to confirm basic system information, including storage settings, access arrangements and technical capabilities. Evidence gathered through early engagement similarly indicated that many services had limited technical knowledge of their CCTV systems and relied on external providers to explain how they operated.[20]

"Some services will say, 'the third-party provider has to give [the footage] to me', so you can't just roll into the service and view it."

Regulatory Authority

Provider size unsurprisingly has an influence on the level of capacity and capability to manage CCTV systems. Larger providers tended to have dedicated operational, facilities or IT functions to support CCTV procurement, installation and upgrades. Smaller providers more often reported relying on external specialists or local networks to access technical capability. School-based services drew on the IT professionals and systems in place for the school.[21] As a result, technical knowledge frequently sat outside the service itself, particularly among smaller providers. This had a practical effect on services' ability to use and maintain their systems well, but also (in a significant minority of cases) to complete straightforward tasks such as to download footage or transfer it to the RA.

In one example, a staff member explained how they used their phone to take a video of the CCTV recording to send to the RA, as they didn't know how to download it. The staff member did not seem aware of the fact that doing so was in breach of the service's policies relating to safe management of potentially sensitive CCTV data.[22] This is consistent with other observations related to a reliance on external expertise, set out in the box below.

[17] Ibid
[18] Service / Centre Manager Survey 1
[19] Site visits
[20] Assessment onboarding
[21] Ibid
[22] Site visits

Reliance on third-party technology providers introduces governance and oversight challenges.

There is a notable information asymmetry between ECEC services and specialist CCTV vendors, particularly where third parties manage the storage, hosting or administration of footage on a service's behalf. While the services retain accountability for how footage is collected, stored and accessed, many lack the technical expertise to critically evaluate their vendor's system architecture, storage practices and access controls. As a result, their ability to independently assure themselves that footage is being managed securely and in compliance with privacy obligations is constrained. This limitation was evident throughout the Assessment, with numerous services referring technical queries to third-party suppliers.[23]

This situation heightens the risk of footage captured within ECEC environments being misused, or of there being inappropriate access to or retention of data beyond intended storage periods. Concerns of this nature were frequently raised by families, although respondents did not always distinguish between risks posed by the service itself and those arising from outsourced technology and support services.[24] Such concerns were also raised by some RAs, who observed instances where services appeared to have only a limited understanding of how footage was stored, accessed and managed by third parties.[25]

While the Assessment did not identify any such incidents, the prospect of highly sensitive footage involving children being improperly accessed or distributed underscores the importance of robust oversight of third-party management arrangements. Without adequate safeguards and accountability mechanisms, these vulnerabilities represent a material risk not only to privacy and child safety, but also to broader confidence in the use of CCTV within ECEC settings.

There are variations in the formality of consent processes and the level of rigour in privacy policies and governance arrangements.

Most services informed families about CCTV use through enrolment materials, sharing of privacy policies and other service communications. One provider we visited used a Parent Advisory Committee to consider and approve the draft privacy policy. That said, services tended to rely more on implied consent: according to one of our surveys, only around ten per cent of those with CCTV had a standard practice of explicitly obtaining parental consent. More than three-quarters notified families about CCTV use through existing enrolment and communication processes.[26] This may not be sufficient to meet regulatory requirements in NSW and the ACT, which have workplace surveillance laws that prescribe additional consent measures. ECEC services in those jurisdictions must provide at least 14 days' written notice and have clearly visible signage at each entrance to the premises.

Knowledge of CCTV access and sharing requirements was often concentrated among a small number of staff. Participants reported inconsistent understanding of external sharing protocols and uncertainty about who was authorised to release footage. In some services, knowledge of CCTV access and disclosure requirements appeared to be held by a few individuals. While it is appropriate to maintain a tight control on access, there were cases of an evident 'key person risk' – for example, not knowing how to access footage for the RA to view during periods when the responsible person was on leave.[27] This points to gaps in the governance arrangements.

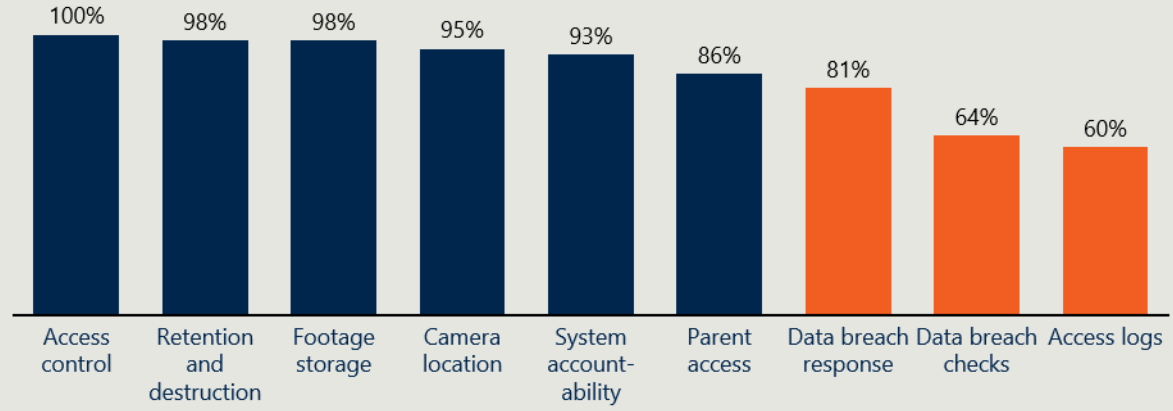
More generally, the Assessment identified issues with the comprehensiveness of key privacy and data management policies. The Assessment conducted a preliminary analysis of nearly 200 policies submitted by 102 Tier 2 and some Tier 1 services and providers as part of the initial expression of interest survey, to

[23] Assessment onboarding
[24] Parent and Caregiver Survey
[25] RA interviews
[26] Sector-wide Survey
[27] Assessment onboarding, site visits

determine the extent to which they cover nine key governance areas of CCTV systems. These nine areas were chosen to reflect key legislative, regulatory and policy documents, including the *Privacy Act 1988* (Cth), the *National Law* and *National Regulations*, and relevant state and territory surveillance and listening devices legislation. The results of that analysis are shown in Figure 5.

In terms of breadth of coverage, policies were inconsistent in the extent to which they included content regarding the risk mitigation and response to data breaches, and the need to log individual access to footage. Smaller, single-site and rural or remote services and providers were more likely to have policies that were inconsistent in their coverage of one or more of the nine governance areas reviewed.

Figure 5 | Extent to which services and providers' policies cover key aspects of CCTV installation and use



Source: Policies of Tier 2 and select Tier 1 services and providers (n=102)

With respect to depth of coverage, the Assessment did not make any judgements, noting that less detailed policies should not necessarily be seen as indicative of a shortfall in meeting regulatory requirements. This is because, while the National Regulations require policies and procedures on the safe use of digital technologies and online environments, including the use of optical surveillance devices,[28] they do not prescribe what these policies must include. The more important question, in the Assessment's view, is whether the policies in place have been fully operationalised to the extent that services and providers can safely use their CCTV systems and effectively manage the associated risks.

On this point, analysis of provider and service-level policies revealed some 'cutting and pasting' of content from generic templates. Around three-quarters of policies reviewed were identified as originating from a policy template, typically sourced from established suppliers such as Childcare Centre Desktop (CCD) and Australian Childcare Alliance (ACA). By comparing policies based on the same template, the Assessment sought to identify what policy content was standardised and what had been developed by providers.

This process identified the following:

- **Templates generally cover relevant CCTV governance principles but often require providers to adopt them as a suite.** Templates consistently addressed core governance requirements including to ensure appropriate camera placement, definition of roles and responsibilities, restriction of access to footage and secure storage. However, these were commonly split across multiple policies, creating a risk of gaps emerging. For example, there were multiple instances where providers submitted a policy based on one supplier's CCTV policy template, which did not cover data breach response processes. This was instead covered in the supplier's Safe Use of Digital Technologies template that the service did not appear to refer to. This was despite the fact that templates also frequently reference related templates. A specific example was noted where a provider's policy stated that "any breach of personal data should be handled as outlined in the Confidentiality and Privacy Policy and Procedure". This related policy was not submitted to the Assessment. Policies also frequently referenced handling of footage in line with more general

[28] *Education and Care Services National Regulations* (Qld), s 168

record-keeping policies without further elaboration. This does not necessarily imply a gap or weakness but underlines the point that the interrelated nature of the policies heightens risks of gaps in coverage in cases where services and providers do not leverage the full suite of templates available from third-parties.

- **Providers inconsistently adapted template content.** There was a wide variation in the extent to which services and providers adapted policies originating from the same template. In some cases, they had not adapted the template at all, as their policies still included unaltered placeholder text (see right). This indicates that use of templates may undermine providers' engagement with CCTV governance issues, leaving policy development as a 'tick-box exercise'. The consequences of this lack of tailoring are described below.

> "CCTV footage is kept in a secure location, located (state location) at the Service for a period of up to [XX days/weeks]."
>
> **Provider's CCTV Policy**

- **Policies inconsistently included important information, including on retention periods and data breach controls**. Retention periods for routine CCTV footage (i.e. footage that does not capture an incident) were inconsistently included in policies developed from templates. This likely reflects the fact that retention periods vary widely between services, placing the onus on them to specify the period rather than rely on template content. Policies that had undergone minimal adaptation were less likely to include retention periods for routine footage. Similarly, policies rarely included proactive data breach controls, such as conducting routine access and download reviews. Instead, policies were much more focused on reactive processes to respond to confirmed data breaches.
- **Where policies did cover governance arrangements, there was not always sufficient detail to operationalise them**. Policies did not always attribute accountability for a governance arrangement to a specific person, job title or role. For example, only about half of the policies named a role or individual responsible for reviewing the policy. Instead, responsibilities like system oversight, access approvals, compliance monitoring and incident response were commonly assigned to the "Approved Provider" or, more broadly, "Management". Similarly, policies usually included a requirement to securely store sensitive footage, including restricting access to authorised users, but provided limited detail on how storage had been secured in practice. For example, policies did not always explain how access is approved, recorded or reviewed. Some policies required an access log to be maintained while others did not.

> "The Approved Provider / Nominated Supervisor / Responsible Person will ensure CCTV is installed and used in accordance with law and this policy."
>
> **Provider's CCTV Policy**

These findings suggest that templates are a useful starting point for providers to develop policies, particularly those who may not feel confident to interpret their legislative and regulatory obligations. However, for some services it can create a 'short-cut' that seemingly compromises the extent to which the policies are fully articulated and operationalised.

A growing number of AI-enabled CCTV systems are available to ECEC services.

Several emerging suppliers are developing AI surveillance products tailored to ECEC environments, with models being trained to identify notable movements and events specific to these settings. However, most remain in the early development or pilot stage, with limited market adoption and little independent validation of their claimed capabilities. The current, more proven, AI features being marketed for use in ECEC settings relate to:

- **Object recognition and tracking:** The AI model is designed to identify people, vehicles and other predefined objects and track their location and movement over time. In ECEC settings, the model aims to identify risks such as phones in rooms, open gates and unauthorised vehicles, as well as alert staff when children enter high-risk areas, approach service boundaries or move into supervision blind spots.[29] The

[29] SooperVision, Every alert. Every risk. Every room., 2025 (accessed 3 August 2026), https://soopervision.com.au/features

model also aims to assess data against established guidelines, such as tracking staff-to-child ratios against National Quality Framework guidance.[30]

- **Unusual activity detection:** The AI model is designed to analyse patterns of movement, behaviour and interactions to identify events that may indicate a safety or wellbeing risk. ECEC-specific providers market this capability as being able to identify events such as falls, rough handling or aggressive interactions, although there is limited public information about how these activity indicators are defined and configured.[31]
- **Automated incident reporting:** The AI model is designed to combine incident detection with natural language processing to automatically generate incident summaries and consolidate supporting evidence. In ECEC settings, the model is marketed as enabling services to automate the preparation of incident reports in formats that meet compliance and record-keeping requirements.[32]

The broader AI surveillance supplier market includes both leading-edge technology companies, as well as traditional CCTV suppliers. Major CCTV suppliers, such as Hikvision, Dahua and Axis, have developed their own proprietary AI models for their camera and video monitoring product lines.[33] Specialist vendors, such as SafeDay, Safe-Sight.ai and SooperVision, package AI capabilities into models purpose-built for ECEC settings.[34]

Reflecting the emerging nature of ECEC-specific AI offerings, use of AI by services participating in the Assessment is concentrated in a small number of early adopters. Section 2.1.2 provides more detail on these.

The regulatory framework for CCTV use in ECEC is complex and not fully aligned.

CCTV in ECEC is regulated through a combination of Commonwealth, state and territory legislation, privacy frameworks, child safety requirements and provider policy obligations. The prime instrument governing CCTV use in ECEC settings is s168 of the National Regulations, which requires services to have policies and procedures regarding the safe use of digital technologies and online environments, including the use of CCTV, and the state and territory Surveillance and Listening Devices Acts. However, there are many other pieces of legislation that relate to CCTV, which can create uncertainty for ECEC services seeking to understand their legal obligations.

This uncertainty has led to instances where services may have unwittingly not complied with the law. For example, the Assessment heard that services in several jurisdictions reported recording audio alongside visual footage, despite surveillance legislation placing restrictions on the recording of private conversations in many Australian jurisdictions. The uncertainty has been exacerbated by gaps, inconsistencies and ambiguities in the regulatory settings across all states and territories, which make it difficult for services to understand their obligations and, for larger providers, to take a consistent approach across jurisdictions.

While not exhaustive, the list below provides some of the Assessment's key findings regarding the prevailing regulatory frameworks related to CCTV in ECEC:

- **Retention of CCTV footage** – There is no specified mandatory period for CCTV footage that does not depict an incident or is needed as part of an investigation or legal proceeding. In practice, this allows services to use their discretion, which has resulted in large variations. The Assessment heard that some

[30] Lunero, Real-time AI detection for childcare rooms, built to work with existing CCTV, 2026 (accessed 30 July 2026), https://www.lunero.com.au/ai-realtime-detection/; SooperVision, Every alert. Every risk. Every room, 2025 (accessed 3 August 2026), https://soopervision.com.au/features
[31] Lunero, Real-time AI detection for childcare rooms, built to work with existing CCTV, 2026 (accessed 30 July 2026), https://www.lunero.com.au/ai-realtime-detection/
[32] SafeDay CCTV, SafeDay CCTV real-time alerts from your existing cameras, 2026 (accessed 30 July 2026), SafeDay CCTV — AI alerts on your existing cameras | SafeDay
[33] Axis Communications, AXIS Object Analytics, 2026 (accessed 30 July 2026), https://www.axis.com/products/axis-object-analytics
[34] SafeDay CCTV, Real-time childcare safety alerts, built for the NQF, 2026 (accessed 30 July 2026), https://safeday.com.au/safeday-cctv/; Safe Sight, AI that cares as much as you do, 2026 (accessed 30 July 2026), https://childcare-info.safe-sight.ai; SooperVision, AI Childcare Supervision Australia, 2026 (accessed 30 July 2026), https://soopervision.com.au/

services do not record footage at all (i.e. only live footage), while others retain footage for longer than 6 months.

- **Rules on camera placement** – States and territories vary in their requirements regarding camera placement. Victoria, New South Wales and the ACT define specific areas where CCTV cameras cannot be placed (e.g. bathrooms, toilets). All other jurisdictions place a ban on recording of a 'private activity' but do not specify areas where a private activity occurs.
- **Consent protocols** – All jurisdictions require ECEC services to obtain consent before using CCTV, but only NSW and the ACT specify what is required to demonstrate that consent has been received (because they have additional workplace surveillance legislation). For all other jurisdictions, it is a matter for services to determine what an appropriate consent process looks like.
- **Treatment of especially sensitive material** – ECEC services are understandably cautious about their obligations when handling CCTV footage that depicts child sexual abuse. Legislation is clear that services cannot be held criminally liable if they capture and share child abuse material with law enforcement as part of an investigation or legal proceeding. However, it is unclear how services should practically and safely share material with authorities, and what additional controls they must have in place to store that footage.

Recently released guidance from the Office of the Australian Information Commissioner (OAIC) provides clarity on two matters relevant to CCTV use in ECEC settings:

1. **Obligations under the proposed Children's Online Privacy Code.** The OAIC's exposure draft of the Online Children's Privacy Code35 may apply to some cloud-based CCTV platforms used in ECEC contexts. This may increase expectations regarding providers' due diligence of technology vendors, including how personal information is collected, used, stored and disclosed, and whether technologies are operating in a manner consistent with children's privacy interests. It may also increase the importance of maintaining clear notices, consent arrangements and governance controls regarding the use of CCTV systems and related technologies.
2. **AI-enabled monitoring and biometric information.** OAIC guidance on Facial Recognition Technology36 emphasises the importance of demonstrating that the use of biometric data (which some AI systems do) is necessary, proportionate and effective. This may require providers to demonstrate that AI-enabled monitoring addresses a significant child safety risk that cannot reasonably be managed through other measures. It may also require providers to validate that AI models are appropriately designed and tested for their intended use, and that sufficient evidence exists to support their effectiveness in delivering intended safeguarding outcomes.

There are implications of the above for ECEC providers' and services' policies and practices in relation to CCTV. These are outlined in Section 3, with supporting analysis set out in Appendix D.

Examples of where RAs have adopted different approaches to leveraging their powers with respect to CCTV use.[37]

CCTV to support proactive regulatory oversight

One RA reported using CCTV footage as part of targeted oversight activities at higher-risk services. Rather than responding to a specific incident, the RA used its authority under Section 197 of the National Law to request footage covering multiple days to observe routine practices, supervision arrangements, and the day-to-day operating environment. The intent was to identify patterns or concerns that may

[35] Office of the Australian Information Commissioner, Privacy (Children's Online Privacy) Code 2026, https://www.oaic.gov.au/__data/assets/pdf_file/0020/262631/Exposure-Draft-Childrens-Online-Privacy-Code.pdf
[36] Office of the Australian Information Commissioner, Facial recognition technology: a guide to assessing the privacy risks, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks
[37] RA interviews

warrant further regulatory attention, enabling a more proactive approach to monitoring service quality and compliance. It is important to note in this context that several services commented that they might have made different decisions about installation of CCTV had they anticipated the extent to which footage could increase their exposure to regulatory scrutiny or legal liability. One service who had volunteered information in the interests of transparency and continuous improvement found that it was unreasonably used against them, souring their view on the value of proactive engagement with the RA.

CCTV as part of a service's provision of education and care

At least one RA has begun treating CCTV systems, where installed, as part of a service's provision of education and care. Under this approach, CCTV equipment may be considered subject to requirements under Section 103 of the National Regulations that "all premises, furniture, and equipment used in providing an …ECEC service are safe, clean, and maintained in good repair." Going forward, establishing consistent application of the National Law by regulators to determine how matters such as this are routinely managed will be critical.

CCTV as a condition of licence

Two RAs noted that installation of CCTV had been imposed as a condition of approval for services to operate. One explained that CCTV had been required to address identified compliance risks, including concerns about supervision and blind spots. Another reported that CCTV had been imposed as a condition of approval for a large provider with a history of compliance concerns. In both instances, regulators emphasised that these arrangements were exceptional and applied only in response to specific risk profiles, rather than representing a standard requirement for service or provider approval.

CCTV in enforceable undertakings

One RA described entering into an enforceable undertaking with a high-risk provider operating two services that already had CCTV systems in place. As part of the arrangement, the provider voluntarily agreed, in good faith, to retain footage for a minimum of four weeks to support future investigations, despite there being no legislative requirement to do so.

2.1.2 CCTV uses in practice

CCTV is primarily used reactively, to investigate incidents or complaints.

The Assessment found that CCTV is predominantly used to support investigations after an incident, allegation or complaint rather than for proactive monitoring. Across participating services, managers were almost twice as likely to report regularly using footage to investigate incidents or clarify what had occurred (67 per cent) than to proactively review footage to identify potential child safety risks or concerns (36 per cent).[38] This view was also evident in how services assessed the value of CCTV: more than half of Tier 2 service managers (52 per cent) identified support for post-incident investigations as CCTV's greatest benefit, substantially exceeding any other reported benefit.[39] Consistent with this, Tier 1 services that completed the withdrawn services survey reported CCTV as most valuable for verifying unwitnessed injuries, investigating complaints and resolving conflicting accounts.[40]

> "We use it a lot for reviewing minor falls or trips in the playground, just so we can ascertain what exactly has happened and how we can support the appropriate responses"
>
> **ECEC Provider**

RAs almost always use CCTV in the same way – that is, to support investigations rather than do proactive checks of footage. Footage is reportedly almost always used (when available) to support investigations by

[38] Service / Centre Manager Survey 1
[39] Service / Centre Manager Survey 2
[40] Withdrawn Services Survey

helping establish an objective account of events, reducing reliance on witness accounts and strengthening the evidentiary basis for regulatory decisions. As one RA explained, "If we have CCTV, it vastly reduces the amount of other evidence that we have to collect". Several indicated that checking whether relevant CCTV footage exists has become a routine step in investigations.[41]

Services' approaches to footage review varied considerably. Some reported a preference for reviewing footage in real time, while others preferred to review footage at accelerated playback speeds to maximise efficiency. One service manager explained that they commonly used playback speeds of up to 8x when searching for a specific event, before returning to real-time speed once the relevant footage had been located to enable a more detailed review of the incident.[42] As part of the Assessment's proactive monitoring and retrospective review, providers/services were asked not to review footage faster than 1.5x real-time playback to ensure consistency.

Proactive monitoring practices were uncommon prior to participation in the Assessment, with only a small number of services reporting that they review routine footage unrelated to a reported incident.[43]

The usefulness of CCTV depends on system configuration and organisational capability.

CCTV's utility varies depending on the camera setup and how systems are configured. Differences in retention periods, storage arrangements, camera coverage and system functionality also influence whether footage is accessible.

Availability of footage

CCTV footage retention periods differed substantially across Tier 1 participating services. Some had no recording capability and so relied on 'live' monitoring. Others had systems allowing them to retain footage for up to three years. The median period reported among services was 30 days.[44] While shorter retention periods reduce storage costs and privacy risks, they can also limit the value of CCTV for investigating incidents, complaints and allegations. One provider reported that a parent requested footage several weeks after an incident, by which time it had already been deleted.[45] RAs reported similar challenges, with footage often unavailable because it had been deleted before review. Although most jurisdictions could not quantify the issue, those that could identified expired retention periods as a common reason footage was unavailable.[46]

Unsurprisingly, camera coverage also influenced the usefulness of footage for investigations. Some services operate extensive camera networks covering most indoor and outdoor spaces, while others focus on entrances, exits and external areas. Again, this was an issue for RAs. One described a case where an incident was recorded but the educator "didn't turn around and face the camera" which complicated the investigation as they were unable to identify the relevant conduct because the footage "was not what was needed to be able to make a clear identification".[47]

System functionality

Not all CCTV systems provide the same investigative value. Differences in storage arrangements and system functionality influence how quickly footage can be retrieved, how easily it can be shared, and whether it is of sufficient quality to support investigations. While around three in five providers stored footage on-site, others relied on cloud-based platforms that enabled remote access and centralised management across multiple services.[48] Services also reported substantial variation in image quality, zoom functionality, search tools and

[41] RA data and interviews
[42] Site visits
[43] Assessment onboarding
[44] EoI Stage 1 Survey
[45] CoPs
[46] RA interviews and data
[47] Ibid
[48] EoI Stage 1 Survey

export capabilities.[49] These differences were evident to regulators, who observed "the quality of what was being provided to support the incident was not what we needed to be able to make a clear identification".[50] Consequently, the effectiveness of CCTV is influenced not only by its presence, but by the technical capabilities of the system itself.

Technical capability

The Assessment found that a substantial proportion of services had a limited understanding of technical features, storage or data export capabilities of their systems.

- **Services had limited understanding of system features:** during onboarding, many services were unable to answer basic questions about their systems, including storage arrangements, cybersecurity practices and technical capabilities such as data export. This was particularly evident among services that had not been directly involved in procuring or installing their CCTV systems. As an example, 30 per cent of providers using cloud-based or hybrid storage solutions (combining cloud and on-premises storage) were unsure whether their CCTV footage was stored within or outside Australia.[51]
- **Knowledge gaps often affected a service's ability to confidently access footage when needed:** it was not unusual for services to report difficulty downloading footage and relied on installers, electricians and IT specialists to explain system functionality or export recordings. This was reflected by services themselves in CoP discussions. One participant explained "I'm not a particularly technical person… when some of the questions came up about the security and what can the systems do, I had to go back to the installer".[52]
- **Regulators faced challenges in accessing and sharing footage:** regulators described instances where services lacked established processes for securely transferring footage and where approaches varied depending on services' technical capabilities.[53]

Technical management can sit outside the service

At this service, CCTV footage was stored and managed as part of the broader building network rather than within the ECEC service itself. When footage needed to be reviewed, service staff relied on the building's central IT team to retrieve and access the recording. While this arrangement provided access to specialist technical support, it also meant that technical administration of the CCTV system sat outside the service itself

Source: site visit of a tier 2 participating service .

> **If we did have an incident… I would just email the IT team or give them a ring and say, can you get me footage from the camera facing the climbing area between this time and that time. Then he'll review it, come over and show me on his laptop.**

Services have adopted different approaches to CCTV governance.

All Tier 2 services had policies related to CCTV governance, but there was no consistent approach in how these arrangements operated in practice. Variation was most apparent in two areas:

- **Access to footage varied between services.** Although services consistently restricted access to a small number of authorised personnel, they differed in how responsibility was allocated and oversight maintained. At some services access was limited to a single individual, such as centre manager or approved providers, while others authorised multiple members of their leadership team. Some services

[49] Site visits
[50] RA interviews and data
[51] EoI Stage 1 survey
[52] CoPs
[53] RA interviews

also implemented additional controls, requiring footage to be viewed by two authorised staff members together.[54]

- **Services adopted different approaches to sharing footage with families**. Some maintained a blanket policy against sharing footage with parents, emphasising privacy considerations and the importance of resolving concerns through established communication processes. Others shared footage in limited circumstances and viewed it as a means to increase transparency following incidents. Community of practice discussions highlighted that parent expectations did not always align with service policies. One provider described receiving a request from a family to view footage following an incident but noted that they had to "resend them the policy and say it's not going to happen".[55]

As a result, services operating similar CCTV footage systems often managed access, disclosure and oversight in markedly different ways.

Services often overestimate their understanding of their privacy obligations.

The vast mast majority of participating services had CCTV in place well before joining the Assessment, and generally had policies in place to govern its use. However, the process of determining eligibility for the Assessment and onboarding services triggered activity among many to complete and update these policies. Experience with CCTV therefore did not always translate into practical understanding of privacy obligations.

Privacy requirements were not always well-understood in practice

As part of onboarding, services were required to complete a Privacy Impact Assessment (PIA). Many services struggled to complete a PIA, often requiring support from installers or IT providers to understand aspects of their CCTV systems. This was evident even among services with longstanding CCTV arrangements. Several providers reported that the process improved their understanding of privacy obligations, with one describing it as an "eye-opener for us".[56]

> "The onboarding process was good…it did point out things like the PIA that we didn't know that we had to have"
>
> ECEC Service

Accordingly, the Assessment found substantial variation in services' capacity to manage data security risks. Some providers described sophisticated security arrangements, including encryption, multi-factor authentication and tightly controlled access protocols. However, these arrangements often depended on access to specialist expertise through technically skilled owner-operators or external advisers. In contrast, other services reported uncertainty about how to securely store, manage and share footage. One provider chose not to expand its CCTV coverage because it was not confident it could adequately manage the associated data risks.

Risks associated with how CCTV data is secured pervade the sector. Concern that footage could fall into the wrong hands was the most common reason for not installing CCTV, cited by 76 per cent of those services without CCTV in an initial sector survey. Throughout Community of Practice sessions and site visits, participants repeatedly raised questions about storage arrangements, access controls and cybersecurity responsibilities.

The Assessment also identified examples where existing practices did not align with privacy expectations. Prior to onboarding, one provider reported that an internal camera had been operating for some time before staff became aware that it captured part of a nappy change area and required adjustment. Another provider also became aware of restrictions on camera coverage late in the installation process, requiring changes to its deployment plans. These accounts highlight that some services had implemented or operated CCTV without fully understanding privacy requirements applied to camera placement or coverage.[57]

[54] Assessment onboarding, CoPs, site visits
[55] CoPs
[56] Assessment onboarding, site visits
[57] Ibid

Privacy obligations were particularly unclear in relation to audio recording. Services in several jurisdictions reported recording audio alongside CCTV, despite surveillance legislation placing restrictions on the recording of private conversations in many Australian jurisdictions.[58] The legality of audio recording depends on factors such as consent and whether a conversation would reasonably be considered private, creating uncertainty about when audio recording is permitted. Several services expressed surprise when these obligations were discussed, suggesting that awareness of audio surveillance requirements was limited. Some regulators also described audio as valuable in investigations, particularly where an understanding of conversations or verbal interactions between educators and children was important to determining what had occurred.[59]

Confidence in privacy arrangements often exceeds demonstrated understanding

While onboarding activities and community of practice sessions identified recurring uncertainty regarding privacy requirements, service managers nevertheless reported high levels of confidence in their own understanding of these obligations. 93 per cent of service managers agreed that their obligations relating to CCTV best-practice safety principles were clear.[60] Similarly, 83 per cent of staff indicated they are familiar with and understand the privacy and legal regulations around the use of CCTV at their service.[61]

The Assessment identified recurring uncertainty regarding camera placement, audio recording and privacy obligations, however.[62] The gaps in understanding also appeared among families: only 58 per cent of parents and caregivers agreed that they understood who was permitted to access CCTV footage. Some parents attributed this to service policies being "long, strangely formatted [and] difficult to follow", making it harder to understand how CCTV footage was being managed.[63]

Privacy risks require ongoing management

The unpredictable behaviour of children creates risks for appropriate recording via CCTV, specifically the risk of inadvertently capturing images of naked or semi-naked children. This risk arises even where cameras are excluded from bathrooms and nappy change areas, because children can be partially undressed in monitored spaces in ways that are difficult to predict or prevent, for example during clothing changes after toileting accidents, during water play, or when young children undress spontaneously.

Some services expressed concern that indoor cameras could capture children in these circumstances, highlighting sensitivities around privacy and dignity. In response, they seek to manage such risks by using software to mask sensitive areas, or to put physical barriers in place (e.g. posters on internal windows or taping part of a camera lens) to minimise uncertainty about what is being captured.

Another feature of ongoing vigilance is being alert to camera positioning. Some services use adjustable cameras that can be re-oriented, creating a risk of someone repositioning a camera to create a blind spot. One service managed this risk through weekly camera alignment checks. [64]

AI-enabled CCTV is concentrated among a small number of technically capable providers.

The Assessment found limited adoption of AI-enabled CCTV among participating services. Five services were included in the AI Scenario for the Assessment, and a composite view based on their experiences is presented in Case Study 4. These providers were typically highly engaged in the technical management of their systems, with service owners or approved providers responsible for configuring, administering and reviewing AI-generated alerts.

[58] Ibid
[59] RA interviews
[60] Service / Centre Manager Survey 1
[61] Staff Survey 1
[62] Site visits, CoPs
[63] Parent and Caregiver Survey
[64] CoPs

All services used CCTV reactively to investigate incidents after they had occurred. However, AI-enabled functionality also supported more proactive monitoring of selected risks by generating automated alerts that enabled real-time response. In practice, these alerts were most used for:

- Perimeter breaches, such as movements across service boundaries or entry and exit points
- Entry into restricted staff-only areas, including offices and storage rooms
- Access to higher-risk operational areas, such as laundries or kitchens
- Potential supervision gaps

More broadly, the AI-enabled CCTV use cases trialled during the Assessment spanned a wider range of child safety, security and compliance-related risks, including:

- **Child safety and supervision:** unattended children, supervision risks, falls and fighting incidents.
- **Security and access control:** unauthorised entry, perimeter breaches, out-of-hours access and persons of interest.
- **Workplace compliance and operational safety:** personal device use, smoking, emergency exit obstructions and location-specific risk areas.

Services using AI-enabled CCTV consistently characterised AI as a supplementary tool rather than a replacement for staff oversight and said it was being used solely to support child safety objectives. Services that did not use AI expressed concerns about the privacy controls around CCTV footage processed by AI.[65]

The use of AI and its effectiveness is discussed in more detail in sections 2.2 and 2.3.

Regional, rural and remote services must be more self-reliant, or pay a premium.

ECEC services outside metropolitan areas have fewer options for procuring, installing and supporting CCTV. The availability of vendors in regional, rural and remote areas is further constrained by the need for them to have Working With Children Checks (WWCCs), causing delays and adding to the coordination burden on services. Some services depend on a single local IT provider for procurement, installation and support, with little competition.[66] Our research found that regional, rural and remote services may pay a 10-20 per cent premium to install CCTV compared to their metropolitan counterparts.[67] This primarily relates to labour costs, which can increase by 10-25 per cent for regional and remote areas,[68] rather than equipment costs.[69] Services in very remote areas are likely to pay the highest premium for CCTV installation, given the more significant logistical and service access challenges they face.

Regional, remote and rural services reportedly respond to these limitations by relying on their own communities. Installation is frequently undertaken by owners, friends or parents with relevant expertise rather than by professionals, who are harder to access. (Note that this phenomenon is not confined to non-metropolitan services.) One service noted that relying on a parent to install their cameras and set up their storage made installation substantially more affordable than using an external supplier. Support appeared to be delivered differently in regional, rural and remote areas compared to metropolitan areas. Vendors typically supported non-metropolitan services remotely through webinars, online training sessions and guidance materials such as pamphlets and user guides, with fewer opportunities for in-person assistance. Participants generally viewed these

> "There was a parent at the service that had done the cameras for a nearby school, so we got him in for a chat"
>
> **Rural ECEC provider**

[65] Assessment onboarding, site visits, CoPs
[66] Ibid
[67] IndexBox, Australia CCTV Camera - Market Analysis, Forecast, Size, Trends and Insights, 1 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-cctv-camera-market-analysis-forecast-size-trends-and-insights/
[68] Built Simple, Electrician hourly rates Australia 2026: state by state pricing, callout fees and how to quote, July 18 2026 (accessed 18 August 2026), https://builtsimple.com.au/blog/electrician-pricing-australia-2026/
[69] Security Wholesalers, Shipping & Delivery Information (accessed 18 August 2026), https://www.securitywholesalers.com.au/shipping/

forms of support as less useful than face-to-face engagement, particularly when addressing technical issues or learning how to use system features.[70]

Such constraints can increase both the cost and effort associated with maintaining and using CCTV. As one regional provider commented, obtaining technical assistance can be a significant burden: "every question costs. It's like billable hours, like solicitors."[71]

Some regional, rural and remote providers with limited financial capacity indicated they would need stronger evidence of its effectiveness before installing CCTV or investing in additional cameras. Despite early interest, some regional, rural and remote services chose not to proceed with participation in the Assessment because of the time, workforce and financial resources required to install systems in time.[72]

Large and small providers adopt different approaches to CCTV governance and oversight.

Provider size influences how CCTV is governed, managed and supported. Larger providers typically operate more centralised models, with responsibility for CCTV distributed across head office functions including operations, facilities and IT teams. While services often store footage locally, head office teams commonly:

- Develop and maintain CCTV policies and procedures
- Oversee procurement, vendor relationships and system upgrades
- Provide operational and technical guidance to services
- Support internal incident investigations
- Engage with RAs when footage is required as part of an investigation
- Oversee risk, compliance and child safety requirements.[73]

As a result, larger providers are more likely to manage CCTV as part of a broader range of their child safety, risk and compliance frameworks rather than as a standalone technology solution.

These arrangements provide larger providers with access to governance, compliance and technical capability that is often unavailable to smaller operators. Interviews with larger providers indicated that many organisations had developed in-house expertise over time, enabling more informed decisions about CCTV design, implementation and its use. Several providers also reported that their scale allowed them to build stronger relationships with vendors and access more tailored support.[74] Consequently, larger providers were generally less reliant on external advice when designing, implementing and maintaining CCTV systems.

By contrast, as noted above, governance, operational responsibility and technical capability were often concentrated in a small number of individuals within smaller providers. Owner-operated services commonly reported CCTV procurement, management, policy oversight and footage review rested with the approved provider or service owner. While some owner-operators demonstrated strong technical capability, particularly those with AI enabled systems, several implemented measures such as encryption, multi-factor authentication and tightly controlled access arrangements.[75] Because of this, the quality of governance arrangements and technical understanding often reflected the expertise available to individual owners rather than organisational systems and processes.

Government-operated services often manage CCTV within broader departmental systems.

Where ECEC services operate within school grounds or under departmental management, responsibility for CCTV installation and footage management often sits outside the service. For example, services reported that CCTV systems in schools are often managed as part of broader departmental infrastructure, with camera

[70] Assessment onboarding, site visits, CoPs
[71] CoPs
[72] Assessment onboarding
[73] Assessment onboarding, engagement with large providers
[74] Engagement with large providers
[75] Assessment onboarding, site visits, CoPs

placement, system configuration and data management determined by school management rather than by the service.[76] Differing legislative instruments may apply to CCTV operating on school sites than to standalone ECEC services. In some jurisdictions, such as Tasmania, school-based CCTV is primarily used for site security purposes and is often focused on external areas rather than learning environments.[77] Because of this, CCTV coverage is concentrated in external areas rather than across ECEC environments.

Governance arrangements relating to footage access were often centralised in these services. In some cases, only the school principal could access footage covering the ECEC service, while in others, access was managed through the school's IT department.[78]

As a result, CCTV implementation is not necessarily straightforward – each of the above can affect the coverage, cost and governance of CCTV systems in ECEC settings.

2.2 Effectiveness of CCTV across child safety outcomes

The effectiveness of CCTV in ECEC settings has been assessed against the Outcomes Framework, which is grounded in the Theory of Change for CCTV use in ECEC settings and the Program Logic developed for the Assessment. This section focuses on the outcomes most directly associated with CCTV use at the service level: detection, response, prevention, and confidence in the sector's use of CCTV.

2.2.1 Detection

CCTV rarely detects incidents or risks that otherwise would not have been observed.

Across the Assessment's reporting period, 80 per cent of the 3,386 incidents (including actual incidents of harm as well as identified issues and risks) were detected through staff observation and 16 per cent through disclosure by children. Only three per cent were identified through CCTV monitoring or review, indicating that most incidents came to light through people witnessing or reporting them.[79]

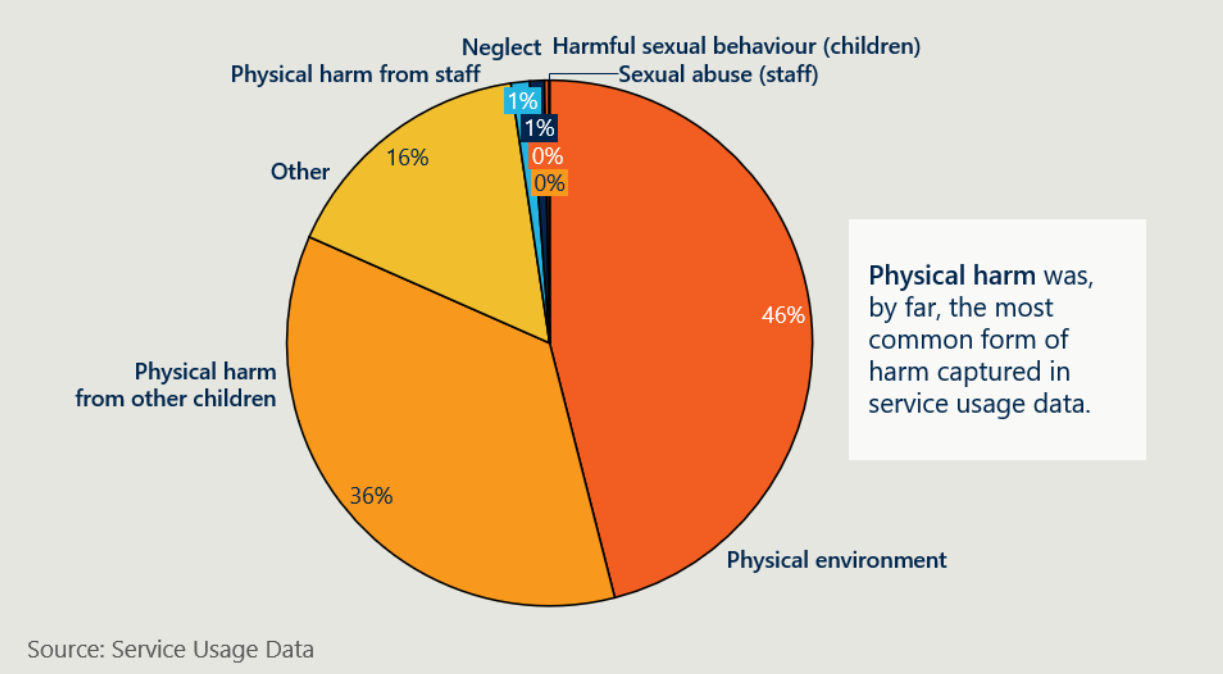
This reflects a fundamental limitation of CCTV: cameras record events, but they typically do not detect something that otherwise would not have been noticed. An exception is AI-enabled CCTV, which can in some cases generate alerts based on predefined risk indicators, and may therefore assist services to identify issues or risks that might go unnoticed.

The distribution of incidents reported through the Assessment provides important context for interpreting these findings. As shown in

Figure 6, physical harm accounted for the vast majority of reported incidents, while neglect and sexual harm were comparatively uncommon.

[76] Assessment onboarding
[77] RA interviews
[78] Loc cit
[79] Service usage data

Figure 6 | Share of harm types among reported incidents



AI-enabled CCTV has higher detection rates, but within a narrow range of circumstances.

The highest CCTV 'detection' rates (defined as per the above description) were reported by services using AI-enabled CCTV. CCTV identified 2.1 per cent of incidents – including issues, risks and actual incidents – in Scenarios 1 and 4 where footage is only viewed (if at all) in an ad-hoc or incidental way, or when an event occurs that requires investigation. This increased to 3.5 per cent in Scenarios 3 and 6, where services undertook proactive monitoring or retrospective review.[80]

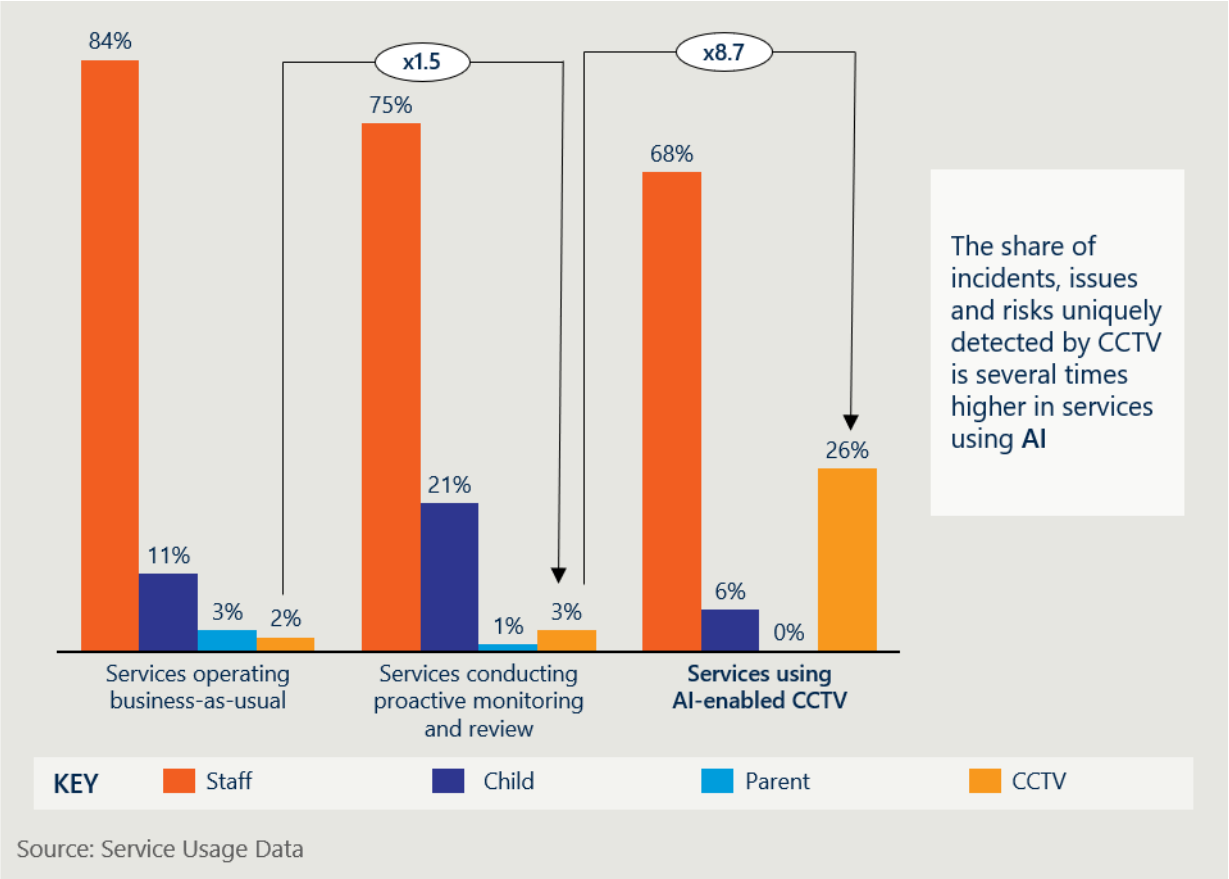
As discussed in Section 2.1.2, AI-enabled CCTV was concentrated among a small number of technically capable early adopters that actively configured, calibrated and managed their systems.[81] Within this group, services reported that 26.5 per cent of incidents were detected through CCTV.[82] This higher 'detection' rate is likely driven by AI-enabled systems generating alerts that prompt staff to review footage, creating more opportunities to identify incidents and risks than conventional CCTV approaches.

However, this finding should not be interpreted as a direct measure of AI accurately identifying incidents. While the reported figure excludes AI alerts that were ultimately determined to be false positives, it does not account for the staff time required to review alerts and determine which warrant further action. Several providers using AI-enabled CCTV described this review process as resource-intensive, meaning the higher detection rate reflects both AI-generated alerts and subsequent human assessment.[83]

The finding should also be interpreted with caution given the small number of AI-enabled services included in the Assessment, which may not be representative of the broader sector.

[80] Ibid
[81] Assessment onboarding, site visits, CoPs
[82] Loc cit
[83] Service usage data

Figure 7 | Share of incident by detection method



Where CCTV does identify issues or risks, they are generally low-level.

More generally with respect to the role of CCTV in detection of an incident, issue or risk, it was more likely to identify lower-level concerns than serious harm. Monitoring or review of CCTV footage most often highlighted supervision issues, environmental hazards such as wet floors inside the service and minor injuries. No incidents involving harmful sexual behaviour between children or sexual abuse by staff were detected through CCTV, although CCTV did identify some instances of physical harm and neglect by staff, consistent with the types of conduct that cameras are most likely to capture.[84]

Overall, incidents detected by services through CCTV were slightly less likely to be reportable incidents (3.0 per cent) compared to those identified through all detection pathways on average (3.4 per cent).[85] Taken together, these findings suggest that CCTV contributes at the service level more to understanding and evidencing low-level incidents and risks to safety than to identifying more serious forms of harm.

The same point applies to RAs, though their focus is naturally on issues and incidents identified through their normal regulatory audit and investigation processes. Interestingly, however, we did hear that RAs regularly detected other 'background' issues or concerns while viewing CCTV, and this was helpful in gaining a broader picture of operations at a service level. In one case, a RA noted that CCTV can assist in identifying or verifying behaviours that precede or sit below the threshold of more serious abuse, including inappropriate conduct, professional-boundary concerns or grooming-related behaviours that may otherwise go unnoticed or unreported.[86] Another RA had found that reviewing several hours of CCTV footage revealed a broader pattern of inappropriate conduct that ultimately supported a decision to prohibit an educator from working in the sector. This finding would not have been reached without access to CCTV data.[87] It should be noted, however,

[84] Ibid
[85] Ibid
[86] RA interview and written feedback
[87] RA interviews

that some services expressed some nervousness about RAs accessing footage for purposes unrelated to a specific, reported incident.[88]

The timing of incidents detected through CCTV closely mirrored the times at which services reviewed footage in Scenarios 3 and 6. Both reviews and CCTV-detected incidents were concentrated in the mid-morning, with a smaller secondary peak in the mid-afternoon. This likely reflects the influence of live monitoring, which can only identify incidents while footage is being actively viewed. In slight contrast, incidents overall were more concentrated in the afternoon, with a smaller secondary peak in the morning.[89] This aligns with the advice of academic experts early in the Assessment, who flagged that more incidents generally occurred mid-morning and mid-afternoon.[90]

CCTV's ability to capture incidents also varied considerably by location. Although outdoor/playground and indoor-room environments accounted for almost 90 per cent of all recorded incidents (53 per cent and 36 per cent respectively), incidents occurring outdoors were substantially more likely to be captured on camera. More than half of outdoor/playground incidents (56 per cent) were fully captured by CCTV, compared to only 40 per cent of indoor-room incidents, while more than half of indoor-room incidents (53 per cent) had no relevant footage available.[91] This difference likely reflects the fact that many Tier 2 participants only had external cameras, but is also consistent with evidence that many minor injuries occur in outdoor play areas.

The benefits of CCTV are amplified when services can proactively review footage.

As part of the Assessment, providers in Scenarios 3 and 6 undertook proactive review of CCTV footage in addition to reviewing footage in response to incidents or concerns. In contrast, services in the other scenarios primarily used CCTV reactively following an incident (excluding the distinct case of AI-enabled monitoring in Scenario 5).

Participating services in the proactive review scenarios were expected to undertake at least two hours of footage review each week. However, review practices varied considerably. Some services conducted short, targeted review sessions of 10-15 minutes, while others undertook longer, less frequent reviews.[92] This suggests that proactive review can be operationalised in different ways, with services adapting the frequency, duration and intensity of review to their workforce capacity, scheduling arrangements and risk management priorities.

While many services in Scenarios 3 and 6 considered this level of review unrealistic under normal operating conditions without additional resourcing, there was nevertheless broad recognition of the value of proactive footage review as a reflective and risk-identification tool.[93] This experience appeared to shape perceptions of CCTV's usefulness, with managers who had undertaken proactive review placing greater value on its ability to identify risks and incidents that might otherwise have gone undetected.

Consistent with this, managers in Scenarios 3 and 6 were substantially more likely than those in predominantly reactive review scenarios to agree that CCTV helped identify supervision gaps (97 per cent vs 78 per cent), near misses (79 per cent vs 56 per cent) and physical safety risks (83 per cent vs 61 per cent).[94]

> "we've been able to identify some coaching needs…the biggest thing for us has actually been supervision points and how we've changed our supervision points"
>
> ECEC Service

[88] Site visits
[89] Service usage data
[90] Interview with Prof Leah Bromfield at Centre for Child Protection
[91] Service usage data
[92] Ibid
[93] Site visits, CoPs
[94] Service / Centre Manager Survey 1

Interestingly, one Tier 2 service was already undertaking activities that the Assessment would classify as 'proactive review' prior to the commencement of the Assessment, using CCTV footage to support reflective practice and service improvement. [95]

For effectively all other services, however, the resource demands associated with regular proactive review were considered unsustainable before and after the Assessment. Workforce shortages were consistently identified as the primary concern, with many currently experiencing recruitment, retention and backfilling challenges. This meant it was difficult to divert staff from core responsibilities to undertake routine footage review. Even where services were able to accommodate targeted reviews during the Assessment period, many considered this difficult to maintain over the longer term without additional workforce capacity.[96]

Managing proactive monitoring and review of CCTV footage at the provider level generally proved impractical.

The Assessment was designed to compare outcomes between services where proactive monitoring and review were conducted centrally at the provider level (Scenario 3) and those where review was undertaken within individual services (Scenario 6). This distinction was intended to test whether the location of review activity influenced the effectiveness of CCTV as a tool for identifying and reducing harm or the risk of harm.

In practice, however, relatively few providers were able to implement a provider-level review model. Providers operating multiple services consistently reported that reviewing footage across several locations was highly resource-intensive and, in many cases, operationally unfeasible. As a result, fewer services participated in Scenario 3 than anticipated, limiting the evidence available to assess differences between provider-level and service-level review approaches.[97]

These findings were reinforced throughout the Assessment, where participants emphasised that effective footage review requires both an understanding of ECEC practice and familiarity with the local service context. Factors such as service layouts, daily routines, staffing arrangements, and knowledge of children and educators can provide important context when interpreting footage, which may limit the extent to which review activities can be centralised across providers with more than one service.[98]

An important caveat is that only two large national providers participated in the Assessment. Providers operating 50 or more services may have greater capacity to centralise elements of monitoring or review within specialist corporate teams, potentially reducing impacts on day-to-day service operations while retaining access to appropriate contextual knowledge.

Risk-based review increased the likelihood of identifying incidents and supervision concerns.

Providers in Scenarios 3 and 6 undertaking proactive review of CCTV footage were able to determine which footage to review and when reviews would occur. As part of this approach, services could undertake either random reviews (i.e. selecting footage at arbitrary times) or risk-based reviews focused on times, locations and activities where incidents were deemed more likely to occur.

To support participating services in their identification of high-risk times, areas and activities, Nous provided guidance informed by academic experts and the NQF Child Safe Culture Guide, highlighting higher-risk locations, activities and times of day.

[95] Assessment onboarding
[96] Ibid
[97] Ibid
[98] CoPs

Table 3 | Summary of high-risk locations, times and activities provided to services in Scenarios 3 and 6

Locations	Times	Activities
Outdoor play areas	Mid-morning (10-11 am)	High movement and transitions
Sleep or rest rooms	Mid-afternoon (3-4 pm)	Competing supervision demands
Staff only or uncontrolled access areas	Transition periods	One-to-one or intimate care

The mix of random and risk-based footage review conducted by services enabled comparison between services that adopted risk-based review approaches and those that selected footage at random. Services adopting a risk-based approach identified noteworthy issues at approximately twice the rate of services selecting footage at random.[99] This suggests that targeted monitoring or review strategies can materially improve both the efficiency and effectiveness of proactive use of CCTV.

Several providers reported that proactive review also helped them identify recurring patterns in when and where incidents were most likely to occur in the context of their service. Some staff noted that these insights improved their understanding of child safety risks within their operating context, and multiple service managers indicated that they intended to continue logging incidents after the Assessment to monitor trends and inform future risk management activities.[100]

> "Proactively reviewing footage gave us an opportunity to have a little look and get a …helicopter view of where staff were at any one point in time, (and to consider) why they were in those locations."
>
> ECEC Provider

Reviewing footage retrospectively appeared to be more effective than live monitoring.

As part of their approach to the proactive review of footage, services in Scenarios 3 and 6 could either monitor footage live or review recordings retrospectively. Service usage data indicated that retrospective reviews identified a noteworthy incident in 11 per cent of review sessions, compared with 4 per cent for live monitoring (noting that session lengths varied as they were also determined by each service).[101]

The higher detection rate associated with retrospective review may partly reflect its greater efficiency. Unlike live monitoring, recorded footage can be viewed at accelerated speeds, allowing staff to review a larger volume of footage within the same amount of time. While services participating in the Assessment were asked to limit playback to no more than 1.5 times real-time, this still enabled 50 per cent more footage to be reviewed, increasing the likelihood of identifying incidents or supervision concerns.

AI alert systems can support detection, but only in combination with human judgement.

AI can bring risks to staff attention sooner than conventional CCTV, but only if staff trust the alerts, with that trust largely dependent on their perceived accuracy. As discussed earlier in this section and in Section 2.2.1 (CCTV uses in practice), services using AI-enabled CCTV reported substantially higher CCTV detection rates than services using conventional CCTV, likely reflecting AI-generated alerts creating more opportunities for staff to identify incidents and risks. Unlike traditional CCTV, which typically relies on someone noticing a concern before footage is reviewed, AI-enabled systems can identify predefined risk conditions and generate real-time alerts. While based on the small sample of five services using AI-enabled CCTV, all respondents from these services agreed or strongly agreed that CCTV had helped identify situations where a child had

[99] Service usage data
[100] CoPs
[101] Loc cit

been harmed, or appeared to have been harmed, compared with around one-quarter of respondents across all services who were neutral or disagreed that CCTV had contributed to identifying harm.[102]

However, as noted earlier, this benefit is highly dependent on alert quality. Excessive false positives can quickly create alert fatigue, causing staff and managers to disregard notifications or lose confidence in the system altogether. One provider reported disabling a detection rule after recalibration significantly increased the volume of alerts, to the point where notifications resembled spam and were no longer operationally useful.[103] Similar challenges were reported by a large multi-site provider that had invested significantly in developing and trialling its own AI-enabled CCTV model tailored to ECEC settings.[104] While intended to automate the identification of potential concerns, the system continued to generate a sizeable volume of alerts requiring manual review.

AI-enabled CCTV systems also require ongoing calibration to be effective in detection.

As noted earlier, the use of AI-enabled CCTV needs more than a "set and forget" approach. Participating services refined prompts, sensitivity settings and detection boundaries in nearly every reporting period to improve performance and better align alerts with their operational needs. Scenario 5 providers reported that small adjustments to prompts and business rules could materially improve detection accuracy and reduce false positives.

As part of this ongoing calibration and management of alerts, providers adopted different approaches depending on the value generated by each alert and the effort required to review it:

- **Alerts with very high false positive rates were ultimately removed when they imposed excessive monitoring burden without delivering meaningful value.** One provider had an alert designed to detect staff looking at their watch (given restrictions on personal device use in ECEC settings) but discontinued the alert after it generated an operationally impractical false positive rate of more than 90 per cent and limited evidence that the behaviour occurred in practice.[105]
- **Other alerts with high volumes were retained where they generated useful evidence.** The same provider noted that they kept an alert for children fighting despite producing large numbers of alerts, as it provided an auditable record that could support later investigations.[106]

Unsurprisingly, AI performance was highly sensitive to environmental conditions. Factors such as lighting, reflections, service layout and unavoidable environmental activity, such as wildlife moving through camera views, could affect detection accuracy and require ongoing optimisation. While refining prompts and business rules was the most common approach to improving performance, providers also adjusted physical environments to reduce false detections. For example, one provider addressed repeated false alerts caused by reflections by repositioning a sheet of paper on a window, improving the accuracy of the detection model.[107]

In line with the trade-off between incident severity and monitoring burden, false positive rates varied considerably across use cases. Providers generally accepted higher false positive rates for alerts associated with more serious risks, particularly where missing a genuine incident could have significant consequences. As a result, these alerts often accounted for a substantial share of review effort, although the effort required to assess individual alerts varied by use case and context. For example, it is often relatively straightforward to determine that a bird triggered a perimeter breach alert, whereas identifying a potentially significant incident within busy footage of a play area may require more time and judgment. Conversely, alerts relating to lower-risk

> "If I've got compelling footage…it's very easy… It often takes a few minutes to show that there's a serious concern. It's powerful"
>
> **Regulatory Authority**

[102] Service / Centre Manager Survey 1
[103] Site visit
[104] Ibid
[105] Service usage data
[106] Ibid
[107] Service usage data

behaviours were typically expected to achieve a higher level of accuracy to justify the effort required to review and manage notifications.[108]

Among the small Assessment sample, we were able to compare the false positive rates across some common, moderate-risk use cases. One of these use cases, unauthorised device usage (i.e. a staff member using their phone), saw false positive rates of between ~5 per cent and 30 per cent among the services using AI-enabled technology. This variation is likely driven by differences in the underlying technology, prompt design and alert preferences, as mentioned in the previous paragraph. Variation was even more pronounced for another use case, perimeter fence detection, where two services reported false positive rates of less than 5 per cent, while another reported a false positive rate of around 80 per cent. Given the continuous calibration undertaken by providers to improve accuracy and reduce false positives, false positive rates generally appeared to fall over time as services refined prompts and optimised alerts for their operating environments.[109]

High reliability appears achievable despite ongoing calibration requirements. While false alerts occurred, providers reported no missed alerts during the Assessment period. One provider that participated for the maximum Assessment duration (16 weeks) reported only a single day of system unavailability, which resulted from a service-wide power outage rather than a failure of the AI-enabled CCTV system itself.[110]

Camera blind spots fundamentally constrain CCTV's ability to detect all incidents.

There was broad appreciation among Assessment participants of CCTV's ability to reduce blind spots within services: over two-thirds of managers (68 per cent) agreed that CCTV helps reduce physical blind spots in rooms or outdoor areas.[111] However, camera blind spots remain a major constraint on CCTV's effectiveness. Across the collection period for service usage data, over 58 per cent of incidents classified as 'no-footage available' (where a reason for this was cited) attributed the problem to blind spots, compared to approximately one per cent involving technical failure.[112] This reflects the wide variation in CCTV coverage across participating services; while some services reported near-complete visibility of key areas, others had more limited coverage.[113] The findings suggest that services with partial coverage were not always capturing the locations where incidents and supervision concerns were most likely to occur, highlighting the importance of both where cameras are positioned and the breadth of CCTV coverage.

Services consistently described reducing camera blind spots as an iterative process rather than a one-off installation decision. One participant characterised it as "an ongoing redesign process"[114], while 22 per cent of service manager respondents reported adjusting camera placement following an incident investigation.[115] The select Tier 1 services engaged through the Withdrawn Services Survey reported similar views, indicating that changes to camera placement occurred in response to incidents, but relatively infrequently.[116]

Services also adapted their physical environments and practices, in conjunction with CCTV camera placement, to improve visibility. Examples included removing roofs from cubby houses, encouraging staff to use transparent materials for forts, and redesigning play spaces to minimise areas obscured from cameras. One service reported that reviewing CCTV footage identified a recurring supervision blind spot near a fort, leading to the installation of a convex mirror to improve sightlines into the area.[117]

Several participants suggested that camera blind spots could be avoided through more deliberate planning at the outset. As one manager reflected, "more thorough conversations… need to take place ... prior to

[108] Ibid
[109] Ibid
[110] Ibid
[111] Service / Centre Manager Survey 1
[112] Service usage data
[113] EoI Stage 1 Survey
[114] CoPs
[115] Service / Centre Manager Survey 1
[116] Withdrawn Services Survey
[117] Site visits, CoPs

installation (because) it is always difficult to increase cameras (or) improve (their placement) after the installation".[118] Together, these findings suggest that effective CCTV coverage is achieved through a combination of careful upfront planning and ongoing refinement informed by operational experience, including consideration of how camera placement interacts with broader environmental design features that support clear lines of sight.

Not all stakeholders see CCTV-based detection of risks as a desirable objective.

There was broad agreement across all experience levels that CCTV can help identify child safety issues or risks, although agreement was somewhat higher among staff with fewer than three years' experience (85–88 per cent) than among those with longer tenure (83 per cent for 3–5 years, 81 per cent for 5–10 years, and 77 per cent for over 10 years).[119]

Discussions with managers suggested that this difference may reflect varying views about the role CCTV should play in identifying risks, rather than disagreement about its usefulness. Several managers described CCTV as a valuable supplementary tool for understanding incidents and concerns but emphasised that effective supervision practices should remain the primary mechanism for identifying and managing risks. As one manager noted: "We have well planned supervision plans and policies and have not had the need to use or review anything until a recent injury that was not captured on CCTV".[120] For these services, limited use of CCTV was seen as evidence that supervision systems were working as intended, and consistent with strong supervision and safeguarding practices.

RAs expressed similar views. While one RA noted that CCTV can assist with initial risk assessment, most indicated that it was rarely used as a broader quality or safety indicator, or as a tool for looking beyond the cause of specific alleged incidents.

CCTV has an apparent positive influence on staff's willingness to report incidents.

ECEC staff consistently reported a process of desensitisation to CCTV surveillance, with awareness of cameras diminishing over time as they quickly became a familiar part of the background environment.[121]

Survey findings nevertheless suggest that CCTV can influence reporting behaviour: 58 per cent of respondents said they were more likely to raise an incident when footage could corroborate what occurred. This effect was strongest among casual staff (69 per cent), compared with full-time (60 per cent) and part-time staff (55 per cent).[122] The availability of footage therefore appears to give some staff greater confidence that concerns can be substantiated and investigated.

In a similar vein, one RA commented that CCTV can increase approved providers' willingness and ability to self-report incidents and compliance concerns that might otherwise go unreported. The RA described instances where providers identified potential breaches of the National Law through retrospective review of CCTV footage and subsequently reported these matters to the RA, highlighting the role of footage in detecting and responding to concerns that may not otherwise have been identified.[123]

Notwithstanding the above findings, the Assessment did not see any evidence of an increased use of 'whistleblower' provisions to report on unsafe or inappropriate practices on the part of individuals or services.

CCTV appears to have a limited effect on whether, or how quickly, families raise concerns following an incident.

The Assessment's findings suggest that CCTV increases families' awareness of footage as a potential source of evidence following an incident but has only a limited influence on the likelihood or timeliness of reporting

[118] Site visits
[119] Staff Survey 1
[120] CoPs
[121] CoPs, site visits
[122] Staff Survey 1
[123] RA interviews

concerns. While 87 per cent of parents and caregivers survey respondents agreed that knowing CCTV was in place made them more comfortable raising a concern or complaint (including 52 per cent who strongly agreed), there is little indication that CCTV materially changes reporting behaviour.[124]

This pattern was reflected in service experiences. Several managers reported that parents who were aware CCTV was installed were more likely to enquire about or request footage following an incident, particularly after discussions about CCTV, reminders that it was in operation, or periods of heightened media attention on child safety incidents involving CCTV. However, services did not see this translating into higher rates of incident reporting or complaints. On the contrary, services regarded external factors unrelated to CCTV as influencing families' propensity to raise concerns. These external factors included, notably, the damage to the reputation of the sector in the wake of publicly reported child safety incidents, which has sensitised parents and carers more to potential risks.[125]

Families with established relationships with a service, including those with older children who had previously attended or longstanding connections with staff and management, were generally less likely to express concerns about the quality of education and care provided. Services reported that these families often had greater trust in the service, particularly in smaller or close-knit communities. Conversely, one service reported that parents enrolling their first child in care were consistently more likely to raise concerns and seek reassurance, regardless of whether CCTV was installed. Together, these findings suggest that family familiarity and trust in a service may have a greater influence on parental concerns than the presence or absence of CCTV.[126]

2.2.2 Response

Where available, CCTV footage has become a key source of evidence in investigations.

By far and away, CCTV is most frequently used to inform investigations of incidents or complaints. Almost half of managers, 46 per cent, reported always using CCTV during investigations, with a further 21 per cent reporting that they often do so.[127] Unsurprisingly, managers most often identified CCTV as valuable for investigating incidents where events were unclear or disputed. Consistent with this, 82 per cent agreed that CCTV helped confirm whether a child had been harmed following a report.[128]

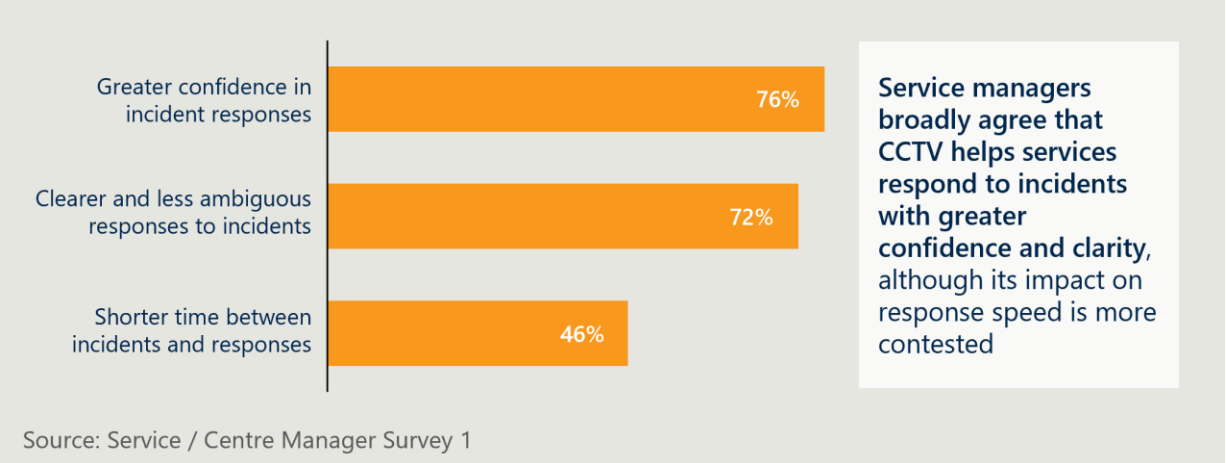
In this sense, the primary value of CCTV appears to be strengthening the evidence base. Eighty-six per cent of staff surveyed agreed that CCTV made it clearer what had occurred during an incident.[129] Several regulators highlighted that CCTV provides a more objective evidentiary source than witness accounts alone. They noted that footage allows investigators to "see exactly what has occurred" rather than rely solely on what people may or may not have seen.[130] This had the effect of substantiating allegations and/or exonerating educators where concerns proved to be unfounded or overstated. One RA also noted that viewing footage can prompt staff facing allegations to amend or clarify their existing accounts, further supporting accurate fact-finding and decision-making.[131]

Among managers of ECEC services, 72 per cent agreed that CCTV helped them to be clear on the appropriate response to identified incidents: 75 per cent reported greater confidence that the correct response had been taken (when footage was available).[132] This perception was echoed by families, who in their survey responses

[124] Parent and Caregiver Survey
[125] Ibid
[126] Ibid
[127] Service / Centre Manager Survey 1
[128] Ibid
[129] Staff Survey 2
[130] RA interviews
[131] Ibid
[132] Service / Centre Manager Survey 1

placed greater value on CCTV as a tool for responding to incidents rather than for preventing or detecting them.[133]

Figure 8 | Service manager views on the benefits of CCTV at their service



RAs described CCTV as being particularly valuable in matters involving educator conduct. One RA noted that "a lot of immediate prohibitions rely on CCTV evidence", observing that footage can support faster regulatory intervention where conduct is clearly visible.[134]

That said, fewer managers of ECEC services agreed that CCTV reduced the time between an incident occurring and action being taken, with 46 per cent suggesting the process of locating, reviewing and interpreting footage may in fact extend investigations, particularly where footage quality makes events difficult to interpret, or where large volumes of footage must be reviewed to identify the relevant timeframe, even where it improves evidence quality.[135]

Of note is that AI-enabled CCTV systems can speed up the process of identifying relevant footage.[136] This capability is particularly valuable when services are attempting to reconstruct an incident, trace a child or staff member's movements across a service, or determine where and when a concern may have arisen. Some AI-enabled CCTV models use biometric data to enable these functions, while others operate without collecting or processing biometric information.

Data retention periods are inconsistent and often poorly understood.

The Royal Commission into Institutional Responses to Child Sexual Abuse recommended that records of child sexual abuse be retained for 45 years.[137] However, there is no specified retention period for routine CCTV footage (i.e. footage that does not capture an incident).

In practice, retention periods for routine footage vary substantially across services. Around 25–30 per cent of providers retain footage for approximately 30 days, while around 10 per cent retain footage for approximately 60 days. Some providers reported keeping footage for as little as two to three days, primarily to minimise storage costs. While others retained footage for considerably longer periods, some reporting upwards of four months. This variation in retention periods applied across geographic locations, service type and size. Very few participating services did not retain footage at all, relying solely on live monitoring. In a significant number of cases, managers and service staff did not know the exact retention periods applied to their system's footage.[138]

[133] Parent and Caregiver Survey
[134] RA interviews
[135] Service / Centre Manager Survey 1
[136] CoPs
[137] Royal Commission into Institutional Responses to Child Sexual Abuse, Final report, Recommendation 8.1
[138] EoI Stage 1 Survey

Retention periods are critical, because the ability of CCTV to support investigations is dependent on whether relevant footage is still available when concerns are identified and reported. While 11 per cent of service manager survey respondents reported receiving requests for footage after the relevant footage had been deleted[139], most often in services with 30-day retention periods, the service usage data suggests that such occurrences were uncommon during the Assessment period[140]. The Assessment found that relevant footage was typically still available when concerns were raised, with 97 per cent of incidents identified on the same day they occurred and a further two per cent within seven days.[141] These findings are not directly comparable, however, as the service usage data captured incidents and requests occurring within the Assessment window, whereas the survey reflected respondents' experiences across their broader careers and use of CCTV.

Taken together, the findings suggest that requests for deleted footage can occur, particularly in cases involving delayed disclosures or emerging patterns of concern but are relatively infrequent. Given that only around one per cent of incidents were reported more than seven days after they occurred, a 30-day retention period appears sufficient to support investigative review in the vast majority of cases, while reducing the costs and privacy risks associated with retaining footage for longer periods.[142]

> **Retention periods affect whether footage is available for formal investigations**
>
> A regulatory authority highlighted the practical challenges created by inconsistent retention practices across the sector noting that *"some services say they only keep it for 48 hours, some keep it for two weeks ... Having some consistency around those sorts of requirements around retention, I think, would be really good."* The same RA observed that short retention periods can limit the evidentiary value of CCTV when concerns are identified after a delay. They suggested that *"if they're aware that there is an incident that's potentially captured by CCTV, they should retain that footage until they're advised that the matter has been closed off by the regulator."*[143]

CCTV can strengthen investigations even when incidents are not directly captured.

The value of CCTV extends to capturing contextual evidence. While footage does not always show the incident itself, providers described using CCTV to reconstruct events, establish who was present and understand circumstances around harm.

Several Tier 1 Assessment participants reported that footage helped piece together what occurred before and after an incident. In these cases, CCTV provided evidence that was not available through witness accounts alone. One provider described using footage to distinguish between accidental and deliberate causes of an injury, despite the injury itself not being clearly visible.[144]

Some providers also used CCTV to understand broader factors affecting child wellbeing. In a small number of cases, footage helped identify changes in a child's behaviour or revealed circumstances that may not otherwise have been apparent.[145]

Stakeholders noted that emerging technologies may increase the ability of CCTV systems to generate contextual insights. Expert panel members highlighted the potential for AI-enabled systems to identify behavioural patterns or activities in settings where camera coverage is constrained by privacy

[139] Service / Centre Manager Survey 2
[140] Loc cit
[141] Service usage data
[142] Ibid
[143] RA interviews
[144] CoPs
[145] Ibid

requirements.[146] However, participants reported limited use of these capabilities and noted that evidence of effectiveness in ECEC settings is still emerging.[147]

Poor quality footage can be an issue for RAs.

The usefulness of CCTV in investigations was also affected by footage quality. Services reported that footage was unavailable in fewer than 1 per cent of incidents across reporting periods.[148] However, RAs, reflecting their jurisdiction over services that have and do not have CCTV, reported greater difficulty obtaining usable footage.[149] Issues affecting usability of footage included:

- Fisheye distortion, which could make it difficult to distinguish between adults and children
- Poor lighting
- Limited zoom capacity
- Limited ability to capture facial features for identification purposes
- The absence of audio

These limitations could make it difficult to identify individuals or understand the circumstances surrounding an incident, even where footage was available.[150]

There are trade-offs in terms of time and value from using CCTV for investigative purposes.

Notwithstanding the value of CCTV as a tool for evidence, several services reported that reviewing footage can be resource-intensive, particularly where incidents require footage from multiple cameras or extended periods to be examined. Service managers observed that while footage often increased confidence in decisions - it could also prolong investigations while evidence was reviewed and verified. [151] Some managers further noted that parents' expectations that footage will be reviewed following incidents created additional time pressures. [152]

These findings suggest that CCTV is more effective at improving the quality and certainty of investigative outcomes than reducing the time required to reach them. Providers consistently described footage as a valuable early source of evidence, helping determine whether concerns warranted further investigation and whether allegations against staff could be substantiated. In some instances, footage also exonerated staff by confirming that incidents or risks involved other individuals. However, CCTV typically didn't provide a complete picture on its own, with witness statements, records and other supporting information typically still required.[153] RAs similarly reported using CCTV primarily to understand and corroborate reported incidents, with footage most valuable when it resolved uncertainty, tested the consistency of different accounts, and strengthened findings drawn from multiple sources of evidence.[154]

RAs indicated that CCTV does not necessarily accelerate regulatory investigations overall, as the time required to obtain, store, review and interpret footage can offset potential efficiencies. However, footage can support faster and more defensible regulatory action where serious misconduct is clearly captured, particularly in higher-risk investigations and matters involving decisions about prohibiting staff. In these circumstances, CCTV provides an objective evidentiary basis for regulatory decisions that may be subject to external scrutiny or review.[155]

[146] Expert Panel Interviews
[147] CoPs
[148] Service usage data
[149] RA interviews
[150] Ibid
[151] CoPs, site visits
[152] CoPs, site visits
[153] Ibid
[154] RA interviews
[155] RA interviews

An unintended benefit is that CCTV footage can occasionally be useful for investigations by other government authorities; some child safety related, and others not.

Services reported instances of using CCTV to support police investigations, workers compensation matters and insurance claims.[156] The use of CCTV to support workers compensation (WorkCover) claims was a noted factor among at least three services participating in the Assessment.[157] Some providers also described CCTV as an important source of evidence when responding to external requests from bodies other than the RA – namely police or child protection authorities.[158]

Where services discussed the use of CCTV in police investigations, these were generally related to property offences such as vandalism and theft.[159] However, some providers also described more significant interactions with law enforcement agencies, including instances where footage was provided to support broader criminal investigations. In one case, a service reported that CCTV footage was requested by the Australian Federal Police to assist an investigation related to terrorism due to external camera coverage.[160]

Services also reported that CCTV footage could be used to support child protection investigations. In some cases, footage was reviewed following concerns about a parent's behaviour at or near the service that was reportable. One described a situation where a child protection agency requested that services review footage to better understand a child's demeanour at a particular point in time as part of an investigation into potential harm or neglect occurring outside the service.[161] Such examples suggest that CCTV footage may, in some circumstances, provide contextual information that supports broader safeguarding and child protection activities.

Some services understandably expressed caution about sharing copies of footage externally due to privacy considerations. Where possible, these services preferred external agencies to review footage on-site, allowing the relevant information to be viewed while limiting broader distribution of recordings containing children, families and staff.[162]

2.2.3 Prevention

CCTV contributes most to safety improvements when footage is actively reviewed to identify patterns and emerging risks.

The strongest evidence of CCTV's preventative value unsurprisingly emerged when services engaged purposefully with their footage. Although as noted above, many services and providers reported that routine review was impractical under business-as-usual conditions, those that reviewed footage as part of the Assessment found they were able to extract useful learnings, as outlined below. Indeed, the Assessment found that the more services were engaged in the Assessment, the more likely they were to consider the potential for CCTV to inform continuous improvement.

[156] CoPs, site visits
[157] Ibid
[158] Ibid
[159] Ibid
[160] Ibid
[161] Ibid
[162] Ibid

Supporting reflective practice and continuous improvement

Examples of where review of footage enabled managers and staff to identify areas for improvement and support professional learning, included the following, to:

- Identify reoccurring supervision gaps, specifically for entry level employees
- Inform staff training and coaching, and prompt discussions about privacy, supervision and risk management.
- Strengthen a culture of continuous improvement
- Diagnose behavioural triggers for children with developmental issues

> "We've offered the staff an opportunity to use that as a reflective tool…they're picking up things that they wouldn't necessarily reflect on or act upon in the moment"
>
> ECEC Provider

For example, one service manager put it: "we've been able to identify some coaching needs... the biggest thing for us has actually been supervision points and how we've changed our supervision." See Case Study 5 for more detail on how CCTV is being used to identify patterns in practice that are not readily visible through incidental day-to-day observation alone.[163]

Identifying specific risks and taking corrective action

Services also reported using CCTV footage to identify safety risks and take corrective action – for example, locating an ant nest after a child was bitten.[164] In some cases, reviewing footage helped managers understand the circumstances surrounding incidents and identify contributing factors that may otherwise have gone unnoticed. For example, one service used CCTV to examine why there appeared to be a disproportionate number of injuries occurring in one area of a playground.[165]

Services with CCTV coverage of car parks similarly described using footage to identify unsafe behaviours during pick-up and drop-off periods. Examples included parents driving with children on their laps or reversing through car parks despite limited visibility. One service reported a marked reduction in parents leaving children unattended in vehicles after installing an external CCTV camera overlooking the car park. Prior to installation, the service had repeatedly reminded families not to leave babies or children in vehicles while dropping off a sibling but observed little change in behaviour until external cameras were installed. Managers said the objective nature of footage made these incidents difficult to dispute: parents generally accepted the evidence, apologised and modified their behaviour accordingly.[166]

Such outcomes were most evident in the Scenarios that required proactive monitoring or review. Among managers of services allocated to Scenarios 3 and 6, 97 per cent reported that CCTV helped identify supervision gaps, compared to 78 per cent across the first general survey of managers involved in the Assessment.[167] Similarly, other service staff participating in Scenarios 3 and 6 often spoke positively about the value of footage review for the purposes of learning and improvement.[168]

It is important to note, however, that some of these responses likely reflect an Assessment effect. Participation in the Assessment prompted structured discussions about CCTV, supervision and risk management in Communities of Practice sessions and site visits that may not otherwise have occurred, and the allocation to Scenarios 3 and 6 would have triggered a deviation from current practice for many of the participating services. Several reported that they intended to continue using the Assessment's reporting template after the Assessment concluded, using it to identify recurring themes, monitor patterns over time and target areas for improvement.[169]

[163] CoPs
[164] Site visits
[165] Ibid
[166] CoPs, site visits
[167] Service / Centre Manager Survey 1
[168] Site visits
[169] CoPs

Proactive review of footage can improve understanding of general risks to child safety.

Purposeful review of CCTV footage can improve services' understanding of where and when child safety risks are most likely to occur. Nearly two-thirds of managers (64 per cent) agreed that CCTV had improved their understanding of where and when child safety risks were most likely to occur, with this percentage increasing to 76 per cent among managers in Scenarios 3 and 6 (which required proactive monitoring and retrospective review).[170] This aligns with earlier findings that the greatest benefits of CCTV arise when services actively engage with footage rather than simply recording it.

Services undertaking proactive monitoring and review looked at footage from both indoor and outdoor environments, with a relatively even split between the two. While the specific room types reviewed could not always be identified due to inconsistent naming conventions across services, reviews generally focused on high-use areas where children and educators spend most of their time. Notably, the rate at which a noteworthy incident was identified was broadly consistent across baby, toddler and kinder rooms, with incidents identified in around 10 to 12.5 per cent of reviews.[171]

In the wake of using CCTV to identify environmental risks, several services reported:

- Redesigning outdoor areas (replacing play equipment that created blind spots)
- Improving sightlines for supervision
- Replacing opaque structures with transparent materials to increase visibility.[172]

All agree that CCTV is an additional tool, and not the most important one for child safety.

Participants consistently emphasised that CCTV should complement, rather than replace, active supervision and professional judgement. Throughout the Assessment, educators and carers, service leaders and RAs described CCTV as a useful tool that can strengthen oversight and provide an evidentiary record when needed, but stressed that responsibility for child safety ultimately rests with staff and established safeguarding practices.[173] Reflecting this view, 83 per cent of staff agreed that CCTV supports (rather than replaces) their professional judgement in child safety matters, compared with only 4 per cent who disagreed.[174]

In the same vein, survey findings suggest that both staff and families regard CCTV as an important component of a broader child safety framework, but not its most important element. While 76 per cent of staff rated CCTV as very or extremely important for child safety, it ranked below other safeguards, including staff screening and background checks (95 per cent), physical environment design (95 per cent), child safety training (94 per cent), staff-to-child ratios (93 per cent) and reflective discussions on child safety practices (91 per cent).[175]

Parents and caregivers expressed a similar view. Although 79 per cent rated CCTV as very or extremely important, they placed even greater weight on staff screening and background checks (98 per cent), staff-to-child ratios (96 per cent), environmental design (96 per cent), staff training (95 per cent) and reflective discussions about child safety (95 per cent).[176]

These findings suggest there is broad support for CCTV as an additional layer of protection, but little appetite for it to displace the human and organisational safeguards that participants regard as the foundation of child safety. Instead, CCTV is generally seen as most effective when used alongside strong supervision, well-trained staff, robust governance arrangements and environments designed to promote safety.

[170] Service / Centre Manager Survey 1
[171] Service usage data
[172] CoPs, site visits
[173] Assessment onboarding, CoPs, site visits, RA interviews
[174] Staff Survey 1
[175] Staff Survey 2
[176] Parent and Caregiver Survey

CCTV is perceived to influence collective practice more than individual behaviour.

Most staff did not view CCTV as materially changing how they perform their day-to-day role. Many participants reported that they already work to professional standards regardless of whether cameras were present, and therefore did not see CCTV as a catalyst for meaningful changes in their own practice.[177] This was particularly evident in relation to interactions with, and supervision of, children. Staff were more than twice as likely to disagree than agree that CCTV had positively affected how they supervise or interact with children (46 per cent compared with 21 per cent).[178] Similar findings were reported by the select Tier 1 services that completed the Withdrawn Services Survey, which generally found that CCTV had limited impact on staff interactions with, or supervision of, children.[179]

Staff held similarly mixed views about whether CCTV reduces unsafe or concerning behaviour more broadly. Only 37 per cent agreed that CCTV had reduced unsafe or concerning behaviours, while 43 per cent neither agreed nor disagreed and 19 per cent disagreed.[180] Together, these findings suggest CCTV is not widely perceived as a driver of individual behavioural change.

Staff were considerably more positive about CCTV's contribution at a service-wide level, however. Most staff reported that their views had become more positive about CCTV improving child-safety practices among (78 per cent) and strengthening accountability for child-safety outcomes (82 per cent).[181] In other words, while they generally did not believe CCTV changed how they personally work, many considered it a tool to improve accountability and practices across the service as a whole.

Parents and caregivers offered a similar perspective. More than half of survey respondents (55 per cent) were neutral when asked whether CCTV had positively influenced their interactions with staff; 30 per cent agreed with this statement.[182] This suggests CCTV is more often perceived as influencing organisational practices and accountability than day-to-day interactions.

CCTV's deterrent effect weakens as cameras become normalised.

Evidence from the Assessment suggests that any deterrent effect on existing staff may weaken over time as staff become accustomed to the presence of cameras. Services with long-standing CCTV systems frequently reported that cameras had become part of the background environment and were no longer 'front of mind' for educators.[183] Several described CCTV as becoming effectively invisible once it had been embedded into routine practice, while others said they lost awareness of camera coverage over time.[184] These observations align with findings from the literature review and consultations with RAs and key sector experts, which suggested that staff can become desensitised to continuous surveillance.[185]

To illustrate this point, the Assessment notes that several services reported incidents of inappropriate discipline occurring in areas covered by CCTV. Notably, these incidents were reported months after camera installation, when staff awareness of surveillance had likely diminished.[186] In some cases, staff provided accounts that differed from what was captured on footage, with CCTV later being used to establish veracity.[187] One example involved footage of a staff member handling a child roughly and disregarding the child's distress, which ultimately led to the staff member's employment being terminated. Importantly, the incident occurred despite the staff member having previously received a formal warning, suggesting that the

[177] Community of Practice sessions, site visits
[178] Staff Survey 2
[179] Withdrawn Services Survey
[180] Staff Survey 1
[181] Staff Survey 2
[182] Parent and Caregiver Survey
[183] CoPs
[184] Site visits
[185] Expert Panel consultations
[186] Assessment onboarding, CoPs
[187] Site visits

presence of cameras alone does not prevent all inappropriate behaviour but can provide an objective record when concerns arise.[188]

Relevant to this point, in consultations with Professor Leah Bromfield Nous was advised that surveillance may prompt individuals engaging in misconduct to adapt their behaviour, including by avoiding camera coverage or shifting to less visible forms of harm.[189] The Assessment found no evidence of such behavioural displacement. However, the absence of evidence is to be expected, as any shift towards less observable conduct would be inherently difficult to identify and measure.

More generally, to the extent that CCTV may act as a deterrent, the literature suggests that it is least effective in relation to impulsive conduct or with highly motivated perpetrators who actively seek opportunities to avoid detection.[190] CCTV's effectiveness as a deterrent is also limited by camera placement restrictions, prohibiting observation in settings where abuse may occur (e.g. bathrooms, change rooms).

Some services believe that CCTV can deter unsuitable individuals from entering the workforce.

Several participants suggested that CCTV may contribute to prevention by deterring individuals who are unwilling to work in an environment where practices can be reviewed. Some services considered its presence to send a clear signal about transparency and accountability for child safety towards prospective employees.[191] This was evident in the case of one provider executive who said that CCTV was mentioned in recruitment interviews to test the reactions of prospective employees. Any sense of concern about this was interpreted as a potential risk indicator.

> "CCTV can deter people who want to be lazy or not put child safety first from entering the workforce."
>
> ECEC Service

While this aspect of CCTV's deterrence effect was not pronounced, one respondent to Service / Centre Manager Survey 2 said that "deterring job applicants who may pose risk to children" was the 'primary value' of CCTV for their service.[192] Another stakeholder noted that the deterrence may strengthen where staff become more aware that footage is regularly reviewed.[193]

2.2.4 Confidence in the use of CCTV

Evidence from the Assessment suggests that confidence in CCTV is shaped less by the presence of technology than how its purpose and use is communicated.[194] However, this view needs to account for the fact that participating services were a relatively more engaged cohort. Broader sector feedback, including from providers that had not installed CCTV, showed more substantial reservations about surveillance, privacy and the role of CCTV in ECEC settings.[195]

Staff perspectives

CCTV is generally viewed positively

Most employees feel protected by CCTV, particularly where workplace leadership and culture is focused on learning rather than micro-management.[196] During site visits, educators rarely expressed concerns about being recorded and often spoke positively about CCTV's role in the workplace.[197] This support was frequently linked to a belief that CCTV protects employees' interests by providing verification of the facts about a

[188] Site visits
[189] Interview with Prof Leah Bromfield at Centre for Child Protection
[190] Nationwide Assessment of CCTV Literature Review
[191] CoPs
[192] Service / Centre Manager Survey 2
[193] Loc cit
[194] CoPs
[195] Sector-wide Survey
[196] Site visits
[197] Ibid

situation. Staff at several services reported proactively asking managers to review footage following incidents when they believed it would confirm that they had acted appropriately.[198]

Further, almost two-thirds of staff respondents (64 per cent) said their experience with CCTV made them somewhat or much more likely to recommend working at a service that uses CCTV, while only around 4 per cent said it made them less likely to do so.[199]

Interestingly, staff survey results suggest that reactions to CCTV vary across workforce cohorts:

- **Casual staff may place greater value on the independent evidence CCTV can provide** in workplace settings where they are less embedded in day-to-day relationships and decision-making. Among staff whose services had installed CCTV before they commenced employment, reactions were positive across all employment types, although casual staff were more likely to report a somewhat or strongly positive response (92 per cent) than full-time (83 per cent) or part-time staff (70 per cent).[200]
- **Prior exposure to CCTV was associated with stronger support**. Staff who had previously worked in a CCTV-enabled service were considerably more likely to respond positively to the presence of CCTV in their service compared to those who did not have previous experience of CCTV (68 per cent compared with 41 per cent).[201]

Based on interviews with staff during site visits, however, support for CCTV can plummet if CCTV is seen to be used for performance monitoring or 'micromanagement'. Indeed, we heard of situations where such experiences had soured educator/carer views towards CCTV. One staff member reported, for example, that a history of real-time surveillance by centre leaders had created lasting distrust among staff.[202]

While it was encouraging to hear that these experiences were in the past, it is important to note that the Assessment sample would likely have a bias towards services that have a more thoughtful approach to CCTV use. Regardless, however, it highlights the need for an appropriate workforce culture and effective leadership that communicates clearly the purpose of CCTV as being centred on child safety concerns.

Further, while attitudes towards CCTV were generally positive among participating services, the Assessment identified ongoing concerns about surveillance, privacy and the role of CCTV in ECEC settings. These concerns were most prominent among some providers, educators, unions and sector representatives, who questioned whether CCTV aligns with children's rights, dignity and opportunities for unstructured play.[203] Responses beyond the Assessment sample frequently raised concerns about privacy, constant observation and the risk that CCTV could create a false sense of security.[204]

Some participants also argued that CCTV addresses symptoms rather than underlying causes of harm, suggesting that workforce capability, effective supervision and appropriate staffing arrangements provided more important safeguarding than surveillance technologies.[205] One survey respondent stated, for example, that it was concerning to see the sector "resorting to CCTV to 'cover ourselves'" rather than focusing on improving staffing ratios and quality of care.[206]

Some staff worry about their recorded behaviour being taken out of context.

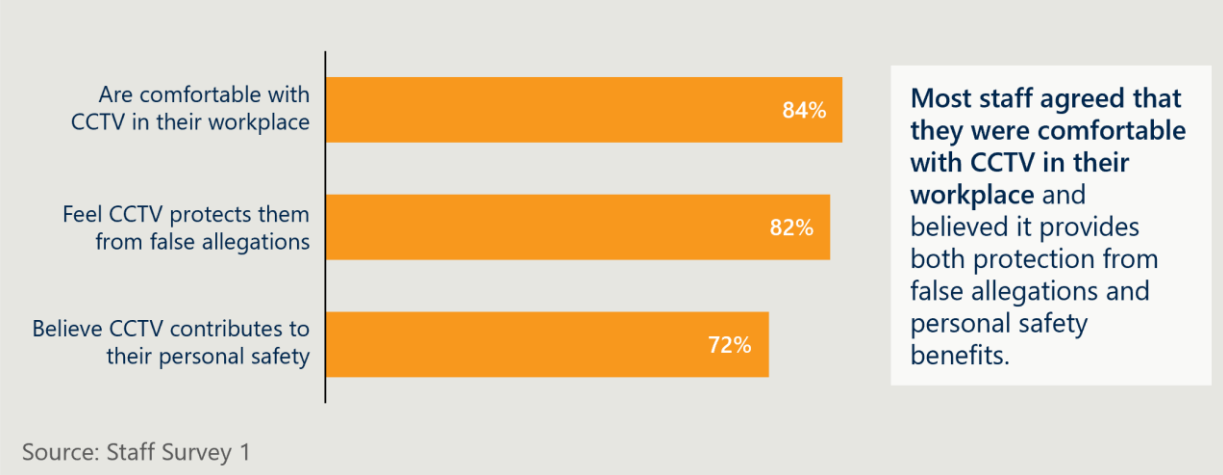
Notwithstanding the generally strong support for CCTV among staff in participating services, a minority held reservations about actions captured in CCTV footage being misinterpreted. Some educators and carers described hesitating during complex interactions with children because they were concerned that appropriate

[198] Site visits
[199] Staff Survey 2
[200] Ibid
[201] Ibid
[202] Site visits
[203] Expert Panel consultations
[204] Sector-wide Survey
[205] CoPs
[206] Ibid

behaviour could appear inappropriate when viewed without sufficient context. [207] For example, one educator noted that staff may feel reluctant to physically intervene to prevent harm or else to provide comfort for fear that their motivations might be misunderstood.[208]

Consistent with this, 18 per cent of managers agreed that CCTV can discourage practices such as messy play or close physical comforting of children.[209] These concerns were particularly evident where CCTV had previously been used as a tool for direct staff monitoring. Across site visits and communities of practice sessions, acceptance was strongest where CCTV was framed as supporting child safety and protecting staff.[210] As noted earlier, most staff reported being comfortable with CCTV in their workplace (84 per cent) and felt it protects them from false allegations (82 per cent). Many also believed CCTV contributed to their personal safety (72 per cent).[211] s

Figure 9 | Staff views on the benefits of CCTV at their service.



Confidence does not necessarily equate to capability. While staff attitudes towards CCTV were generally positive, only 60 per cent reported that training had adequately prepared them to use CCTV within their role, with lower confidence reported by casual staff and some more experienced educators.[212]

Of note, a small number of male staff members whom we engaged in the Assessment and their employers described CCTV as providing reassurance to families about their role in caring for children. One male educator described actively positioning himself in sight of cameras when interacting with children "as a protection."[213]

Family perspectives

Families are also broadly supportive of CCTV

Survey findings indicate that most families understood the rationale for CCTV installation, with 91 per cent agreeing that they understood why their child's service had installed CCTV, including 61 per cent who strongly agreed.[214] Managers' perceptions aligned with this, with around 78 per cent agreeing that parents and caregivers were pleased their service had CCTV, while the remainder were neutral.[215]

[207] CoPs
[208] Site visits
[209] Service / Centre Manager Survey 1
[210] Community of Practice sessions, site visits
[211] Staff Survey 1
[212] Ibid
[213] Site visits
[214] Parent and Caregiver Survey
[215] Service / Centre Manager Survey 2

Notably, providers frequently reported that prospective families asked about CCTV during enrolment tours and viewed its presence as evidence that services were taking child safety seriously.[216] Several services observed that interest increased during periods of heightened media attention and softened as those issues became less prominent.[217]

Some services reported that a subset of parents expected CCTV to provide continuous visibility of their child, often assuming this was an option where CCTV was installed. These parents were generally understanding in situations where privacy requirements made this impractical (i.e. no cameras allowed in the area) or inappropriate (i.e. to protect the privacy of other children). Parents could also be understanding about the resource burden associated with footage requests. For example, one service reported that a parent withdrew their request after learning that reviewing the relevant footage would require approximately three hours of staff time.[218]

More than 80% of respondents agreed or strongly agreed that the presence of CCTV cameras made them feel their child was safer. Only 5% disagreed or strongly disagreed.

Parent and caregiver Survey

To the minimal extent that parents or caregivers opposed CCTV, concerns typically centred on privacy, data security and the potential misuse of recorded footage, with several responses reflecting a low level of trust in services' ability to adequately secure CCTV systems. As one parent commented, "I am a cybersecurity professional and am very familiar with the complexity involved in securing such systems. I have no confidence that sufficient controls are in place to meaningfully secure these cameras."[219] Of note is that these were parents who nevertheless enrolled their children in ECEC services with CCTV.

Such concerns were not evenly distributed across the sector. For example, First Nations representatives highlighted negative experiences of government surveillance and monitoring and the heightened sensitivities, therefore, about how CCTV footage might be misused.[220]

Assessment participants have found effective ways to communicate CCTV to families.

Services reported that concerns dissipated once families understood why CCTV was being used, who could access footage, and what safeguards were in place to protect privacy. One provider reported that only one family among 110 enrolled families had sought additional information following the introduction of CCTV.[221]

Absence of effective communication can have the reverse effect. An example of poor practice was provided in a survey response from one parent: "When my son had a fall and bumped his head, they would not let me see CCTV and gave me no reason why. I felt they were hiding how bad the fall actually was or how it happened."[222] This anecdote illustrates how a lack of clarity about CCTV privacy obligations and access arrangements can contribute to mistrust when incidents occur.

It appears that smaller services are better positioned to both ensure there is sufficient information provided and that trust in the use of CCTV is established. Eighty-one per cent of parent and caregiver survey respondents whose children attended a service with fewer than 50 children agreed that they had opportunities to ask questions or raise concerns about CCTV, compared to 72 per cent of those using services with 50–100 children and 68 per cent with more than 100 children.[223] (A similar pattern was evident among staff, with those in smaller services more likely to report that their views were considered to a 'great deal' during the CCTV installation process – 44 per cent, compared to 31 per cent in larger services.)[224]

[216] CoPs, Site visits
[217] Ibid
[218] Ibid
[219] Parent and Caregiver Survey
[220] Expert Panel consultations
[221] CoPs
[222] Parent and Caregiver Survey
[223] Ibid
[224] Staff Survey 2.

Information needs differ between communities. Some providers serving culturally diverse and lower socioeconomic communities reported that families were often more concerned about photography, digital sharing and online safety than about CCTV surveillance specifically. These services said that strong relationships with families and transparent communication were critical to maintaining confidence in the use of technology-enabled safeguarding practices.[225]

It is important to note that the Assessment was unable to gather sufficient evidence to inform advice on best practice approaches for engaging with First Nations families and communities about the use of CCTV in ECEC settings. While interviews conducted during the Assessment highlighted the relevance of historical experiences of surveillance, cultural safety considerations and issues of data sovereignty, these themes were not able to be explored in depth. The separate evaluation is expected to provide more commentary on these issues.

2.3 Costs of CCTV use

2.3.1 Installation costs

CCTV installation costs vary greatly and are not always proportional to the number of cameras.

Most services in Tiers 1 and 2 of the Assessment reported spending more than $10,000 to install CCTV, but the level of investment varied greatly, and was not always proportionate to the size of the service concerned. Several smaller services reported that they spent as little as $1,000 on installation costs, while a handful of medium-sized ECEC providers estimated costs to be in the order of $20,000-$30,000 per service. However, one service with around 120 children invested over $70,000 for a system with some 60 cameras. One large provider suggested that it generally cost them approximately $40,000 to install a CCTV system with 30 cameras.

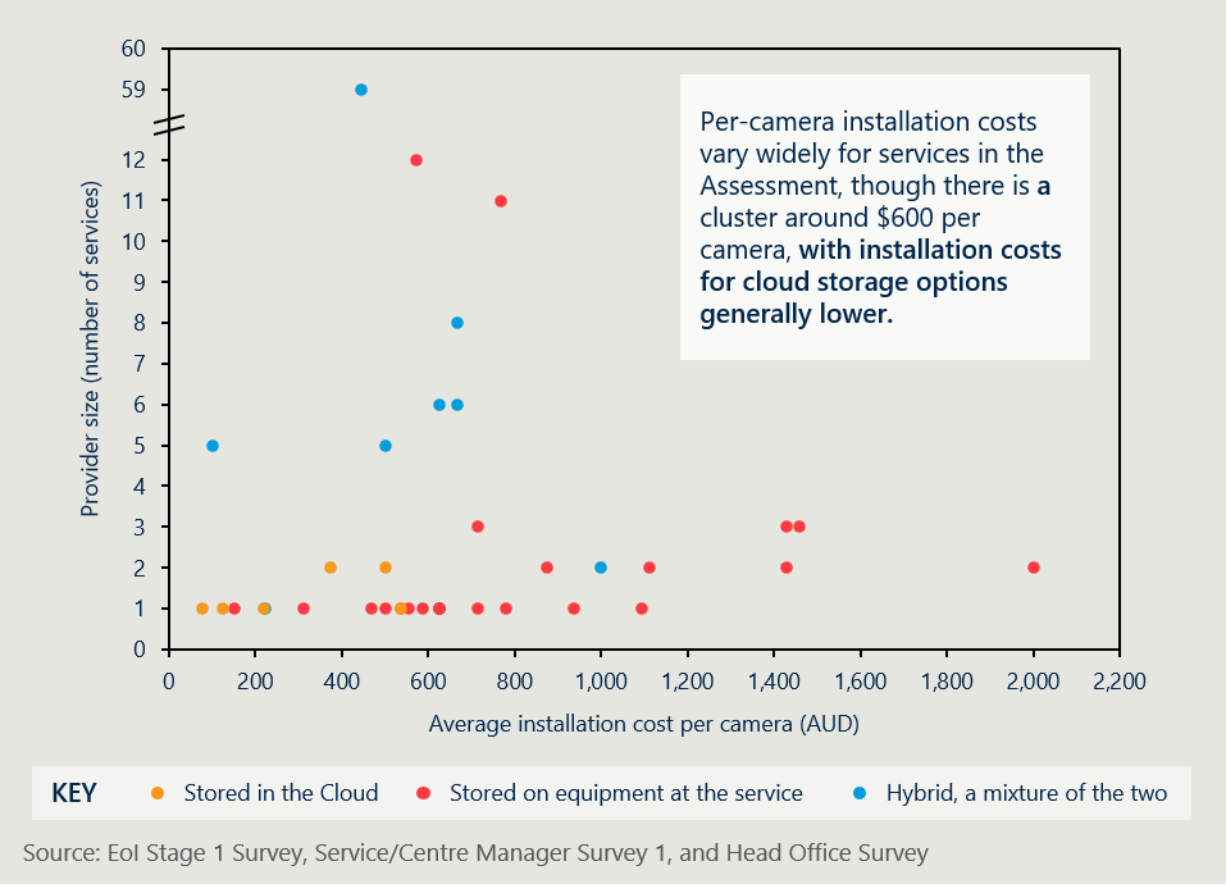
In contrast, there is a clear relationship between installation costs and storage type; more than half of ECEC services in the Assessment using on-premises storage reported installation costs greater than $10,000, compared to fewer than one in five providers using cloud storage.

This reflects the trade-off between upfront and ongoing costs. Physical storage options can carry significant upfront hardware and installation costs. The upfront cost for an 8-channel physical storage unit, excluding hard drives (which are typically sold separately), ranges from around $80 to $400 for DVRs and $250 to $850 for NVRs, depending on storage capacity and number of camera channels.[226] Storing footage from eight 6MP cameras for 30 days generally requires at least 12TB of hard drive storage, which costs around $900 to $1,200 ($75 to $100 per terabyte).[227] However, the ongoing costs of physical storage are typically minimal, except for occasional maintenance or subsequent decisions to expand storage.

Conversely, cloud storage services have lower upfront costs but ongoing subscriptions can be costly. Ongoing costs depend on the number of cameras, choice of continuous or motion-triggered storage, storage duration, video resolution and add-on features. For a system of eight cameras, cloud storage of continuous 6MP resolution footage for a 30-day period costs around $150 to $180 per month. Shorter retention periods carry lower ongoing costs, which can be attractive for small services, but may not be sufficient to support investigations of incidents.

[225] Site visits
[226] Indicative NVR and DVR pricing was derived from a review of available offerings from Australian equipment wholesalers.
[227] Require storage was derived from online surveillance storage calculators, assuming H.265 video format and 15 frames per second recording. Indicative hard drive pricing was derived from a review of available offerings from Australian equipment wholesalers.

Figure 10 | Average installation cost per camera by provider size and storage option



Source: EoI Stage 1 Survey, Service/Centre Manager Survey 1, and Head Office Survey

Note that analysis in this section assumes that services purchased CCTV systems, rather than it already having been installed prior to securing a tenancy. The Assessment also conducted research on the price and feasibility of renting CCTV cameras to enable short-term or periodic use, such as to inform an audit. The Assessment found that the rental market is overwhelmingly comprised of outdoor cameras, often mounted on poles or towers, and intended to be used on construction or mining sites. This is likely to be less suitable for ECEC settings, where the placement of cameras would be preferable, and where the presence of a camera tower in an outdoor play area might present additional physical and psychological safety risks for both staff and children.

Cameras and hardware account for the largest share of installation costs.

This variation in installation costs likely reflects a range of factors. Installation costs are driven primarily by upfront capital expenditure, particularly investment in cameras and associated hardware. Installation labour was consistently identified as the second-largest cost component, while CCTV design, camera placement and software setup contributed comparatively less, with software and licensing costs generally representing the smallest share of upfront expenditure. Table 4 outlines providers' self-reported ranking of each cost component of installation.

Table 4 | Relative influence of installation cost components on overall CCTV system cost[228]

Installation cost component	Average ranking among providers
Cameras and hardware	1.3
Professional installation labour	2.4
CCTV placement/design planning	3.9
Internet/network upgrades (e.g., improving bandwidth or upgrading cabling)	4.0
Local storage (e.g., servers)	4.4
Software/licensing set-up (e.g., setup of monitoring software)	5.1

Camera and hardware

Equipment costs represent the largest component of overall installation costs, with prices predominantly determined by camera features and specifications. The Assessment identified two key features and specifications that affect cost, described below:

High resolution fixed cameras are more affordable than motorised pan-tilt-zoom (PTZ) alternatives and are similarly effective in most indoor environments. PTZ cameras can dynamically adjust their field of view and zoom to follow movement. In contrast, fixed cameras, including turret, dome and bullet types, are set to a predetermined viewing angle during installation. Some higher-cost fixed models can zoom, but they do not offer motorised repositioning. PTZ functionality and motorised zoom increase costs and are typically only justified in large outdoor environments, such as playgrounds or car parks. Where zoom is not required, higher image resolution can achieve similar coverage outcomes, with options ranging from 2MP (1080p) in low-cost models to greater than 8MP (4K) in premium cameras.[229] Professional installers advised that installer-provided cameras typically start at 6MP resolution and cost around $200 to $300 per camera, with optional 8MP/4K resolution adding around 30 per cent to the camera cost.

Wired, Internet Protocol (IP) cameras are more costly than traditional analogue options but enable cloud storage, and advanced monitoring and recording features. Analogue cameras transmit footage using coaxial cables directly to a digital video recorder (DVR). IP cameras transmit footage using ethernet cables (wired) or Wi-Fi (wireless) to a network video recorder (NVR), stream directly to the cloud or store footage within the camera itself on a MicroSD card. IP cameras comprise 70-80 per cent of imported cameras in the Australian market.[230] The upfront cost of an IP camera is typically greater than an analogue alternative, but they are preferred in modern installations for supporting direct cloud storage, remote video access and AI-enabled video monitoring features. When comparing wired and wireless IP cameras, the former typically offer a more reliable, secure connection and power supply, but the cabling installation can be costly, as detailed below. Wireless options are usually more affordable and easier to install, but internet or remote power outages, such as flat batteries, risk disrupting the continuity of footage. Batteries for a Wi-Fi-enabled wireless camera cost up to $80 and usually need to be replaced every two to three years.[231] For larger installations, wireless options may also require Wi-Fi extenders to ensure adequate coverage.

[228] Service / Centre Manager Survey 1
[229] CCTVShop, CCTV Camera Prices Australia, June 2026 (accessed 28 July 2026), https://cctvshop.com.au/pages/cctv-camera-price-guide
[230] IndexBox, Australia Surveillance Camera - Market Analysis, Forecast, Size, Trends and Insights, 3 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-surveillance-camera-market-analysis-forecast-size-trends-and-insights/; IndexBox, Australia Cctv Camera - Market Analysis, Forecast, Size, Trends and Insights, 1 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-cctv-camera-market-analysis-forecast-size-trends-and-insights/
[231] Reconeyez, Wireless security camera battery life and maintenance, 2026 (accessed 28 July 2026), https://reconeyez.com/knowledgebase/how-long-does-a-security-camera-battery-last/

Further detail on variations in camera features and specifications across different price points can be found in Appendix C.

Installation labour

Services reporting installation labour as their largest cost were almost exclusively smaller operations. Consultations suggested the reliance on external installers was particularly challenging for services in rural, regional and remote areas, where appropriately skilled tradespeople can be difficult to source. Installation is further complicated by the need to conduct much of the work outside operating hours, as services typically prefer camera installation and related works to occur when children are not present.

Smaller services may be able to adopt more informal installation approaches, such as purchasing equipment directly from retailers and undertaking relatively simple or 'DIY' installations. Self-installation of low-cost, off-the-shelf solutions can significantly reduce the cost of installation. However, there are risks and downsides associated with a DIY approach. Installation of wired cameras typically requires a licenced professional to run the cabling, which largely limits services to wireless cameras. Furthermore, self-installers may not have the training and experience to position and configure cameras in line with CCTV placement requirements. For example, the Assessment heard of cases where services were using doorbell cameras to capture activity in large rooms and relied on friends or family to install cameras rather than using an electrician.

Other services, particularly larger providers, may choose to outsource system procurement, installation and monitoring to an external security supplier. Professional installers advised that installation costs range from around $110 to $170 per hour, with installation duration dependent on the building specifications and cabling complexity. Select providers also offer ongoing monitoring services of automated alerts, ranging from around $60 to $80 per month, and managed cloud storage services, where providers handle background administration of the cloud, charged at a small premium on existing cloud storage costs. Larger providers are also better positioned to achieve economies of scale by securing discounted bulk purchases, leveraging preferred supplier arrangements, and spreading procurement and implementation costs across multiple services. That said, many large providers have yet to implement CCTV across most or all of their network, meaning the full benefits of scale are unlikely to have been realised.

Installation costs and system scalability are shaped by site characteristics.

While cameras and installation labour represent the largest capital expenses, site characteristics are often the primary determinant of how expensive an installation becomes. The list below outlines some of the site characteristics that can materially affect installation costs:

- Larger services typically require more extensive camera coverage (often meaning more cameras if the provider is seeking near-universal coverage), cabling and supporting infrastructure, increasing both equipment and installation labour costs.[232]
- Purpose-built centres often have better CCTV coverage because they were designed with visibility in mind, often providing clear natural lines of sight and fewer blind spots. By contrast, providers operating from converted houses, heritage buildings and multi-storey premises reported greater challenges achieving comprehensive coverage due to room configuration, internal layouts and reduced visibility between spaces. The limitations of the building layout therefore typically require additional cameras, increasing installation costs.[233]
- Retrofitting CCTV into older buildings is generally more expensive than incorporating systems into new developments, due to physical constraints such as double-brick walls and limited access to existing infrastructure. Services frequently cited additional electrical work, cabling requirements and infrastructure upgrades as contributing to higher installation costs. As one provider explained, "A large amount of the cost was to do with labour because they had to drill through double brick... a 100-year-old house

[232] CoPs, site visits
[233] Ibid

basically." Physical constraints can also make it more difficult and costly to extend CCTV coverage to outdoor areas, particularly where additional power, cabling or connectivity infrastructure is required. In some cases, retrofitting older buildings may be prohibited, creating additional challenges.[234] One instance of this is described in the callout box below.

Challenges of ensuring compliant CCTV installations in heritage buildings

One participating service had a legacy CCTV system installed several decades ago in a location that captured the entrance to bathroom areas housed in a separate building. This provided partial visibility into those private areas. The system, which did not record footage and only displayed real-time vision on a dedicated monitor, was intended to address supervision challenges associated with the design of a converted heritage building, and had been installed on the advice of the RA. In this case, the building's physical constraints made alternative supervision measures impractical, and heritage protection requirements prevented changes to the buildings themselves. The arrangement was considered to reflect an appropriate balance of risks at the time and a justifiable 'exception to the rule'. While this was an isolated example in the Assessment, it may have broader relevance for services operating from historical sites.[235]

- In leased premises, landlords may retain ownership of installed CCTV infrastructure, reducing the service's ability to manage the coverage of its service. Where landlords own the infrastructure, services face collaborative decisions about upgrades or removal at lease end, with reports of unclear responsibility for maintenance. Landlord approval can also influence whether CCTV is installed and the type of infrastructure selected.[236]
- Services operating within community hubs reported that existing CCTV systems were designed to monitor shared areas and protect property, rather than support the specific child safety and operational needs of ECEC services. Extending or modifying these arrangements may require approval from facility managers and consideration of the differing needs of other occupants, limiting a service's ability to independently determine CCTV coverage and functionality.[237]

Services are often required to buy cameras in fixed packages or sets (e.g. 8, 12 or 32 units). These packages can add to installation costs because they may not align with the specific coverage requirements of a service. A service may need to distribute a limited number of cameras across a large area or purchase more cameras than needed. Any additional cameras or hardware must also be compatible with the existing system, which can constrain future expansion and limit flexibility in system design.[238]

As noted previously, CCTV implementation is often iterative rather than a one-off investment. One service reported spending approximately $6,000 on its initial installation before investing a further $10,000 four years later to expand coverage from nine to fifteen cameras and upgrade existing equipment.[239] This later investment included new hardware, installation labour, electrical works and software configuration, highlighting how capital expenditure can continue over time as systems are expanded, modernised and adapted to evolving operational requirements.

Providers also emphasised that early infrastructure decisions can have long-term cost implications. Several noted that older network video recorders (NVRs) can limit opportunities to expand camera coverage or create compatibility challenges when integrating newer camera models, potentially necessitating costly upgrades or replacement of existing equipment. As a result, decisions made during the initial installation phase can affect

[234] Ibid
[235] CoPs
[236] Site visits, Community of Practice sessions
[237] Ibid
[238] Ibid
[239] Ibid

both the scalability of the system and the level of future capital and operational expenditure required over its lifespan.[240]

ECEC services incur additional costs to integrate AI features into their CCTV systems

ECEC services face additional costs to enable AI features. First, AI relies on an internet-connected camera system with sufficient resolution to operate effectively, which may require services with traditional analogue systems to upgrade their hardware.[241] Other requirements depend on the way that AI is integrated into the camera system. In general, AI is either enabled through 'edge AI', hosted on-premises within cameras themselves, on the local recorder (NVR) or as an extension within the local system, or 'cloud AI', hosted on remote servers. The design, requirements and cost of each approach is described below:

- **Edge AI cameras**: An AI-enabled camera processing chip can detect, count and recognise footage contents and transmit only relevant metadata, alerts and clips. AI-enabled cameras can conduct facial and vehicle recognition, person and object tracking, wide area monitoring and behaviour analysis. Use of edge AI, rather than a cloud-based AI platform, reduces the need for a stable, high-speed internet connection. AI-enabled cameras can continue to perform AI functionality without an internet connection if they have on-board MicroSD storage or a wired connection to an NVR, excluding any remote alerts or viewing. An entry-level edge AI camera that detects and categorises motion costs around $230, while cameras containing deep learning analytics and advertised for use in education, healthcare and commercial settings range from $1,500 to $1,900.[242]
- **Edge AI NVRs**: Unlike AI-enabled cameras, where the footage is processed in the camera itself, an NVR can act as a centralised analysis unit that can cross-check footage across multiple cameras to build a full view of an event. Some NVRs, such as Hikvision's AcuSense NVR, connect to an AI-powered natural language interface where users can search for anomalies with image or text input. These systems typically require substantial local storage, wired network connections and large network bandwidth to transmit uncompressed video from cameras to the NVR.[243] Like edge AI cameras, edge AI NVRs can also perform most AI functions without an internet connection. AI-enabled NVRs with motion detection functions cost around $300, while more advanced options that include natural language image and text search functions can range from $1,000 to $2,300 depending on the number of channels supported and video storage capacity.[244]
- **Other edge AI extensions:** Services wanting AI capabilities without upgrading their existing system infrastructure can purchase local AI extensions. These extensions typically come in the form of a physical AI box or virtual AI software installed on local systems, all capable of performing AI tasks without replacing existing system hardware or uploading footage to the cloud. Prices of AI hardware and software extensions vary greatly due to the emergent nature of the sector, often dependent on compatibility with the existing surveillance system.
- **Cloud AI**: Internet-connected cameras can transmit video footage to a third-party AI-powered video management and monitoring platform, where cloud-based analytics are used to detect events, generate alerts, and support video search. Unlike edge AI, cloud AI relies on a reliable internet connection and sufficient bandwidth rather than local AI-enabled hardware. While cloud AI offers benefits such as externally managed software updates, centralised management, and scalability across multiple sites, AI alerts may be subject to network latency.[245] Suppliers may bundle AI features into cloud storage and video management subscriptions or offer them as separate add-on services. A third-party subscription

[240] Ibid
[241] IcetanaAI, Do You Need to Replace Your Cameras for AI Surveillance?, 31 July 2026 (accessed 4 August 2026), https://www.icetana.ai/blog/do-you-need-to-replace-cameras-for-ai-surveillance
[242] Indicative AI camera pricing was derived from a review of available offerings from Australian equipment wholesalers.
[243] Jubo Technology, Edge AI Box vs. AI NVR: Which is Better for Your Security Upgrade in 2026?, 2026 (accessed 5 August 2026), https://aibox-factory.com/blog/tech-insights/edge-ai-box-vs-ai-nvr/
[244] Indicative AI NVR pricing was derived from a review of available offerings from Australian equipment wholesalers.
[245] Controltech Security Solutions, AI Security Cameras: Are they worth it for Australian Businesses in 2026?, 2026 (accessed 25 July 2026), https://controltechsecurity.com.au/ai-security-cameras-are-they-worth-it-for-australian-businesses-in-2026/.

bundling cloud storage, remote management and AI analytics together can cost $45 to $85 per camera per month, depending on footage quality and retention.[246]

See Appendix C on the market for CCTV products and services for more information on the options available for different types of cameras and systems.

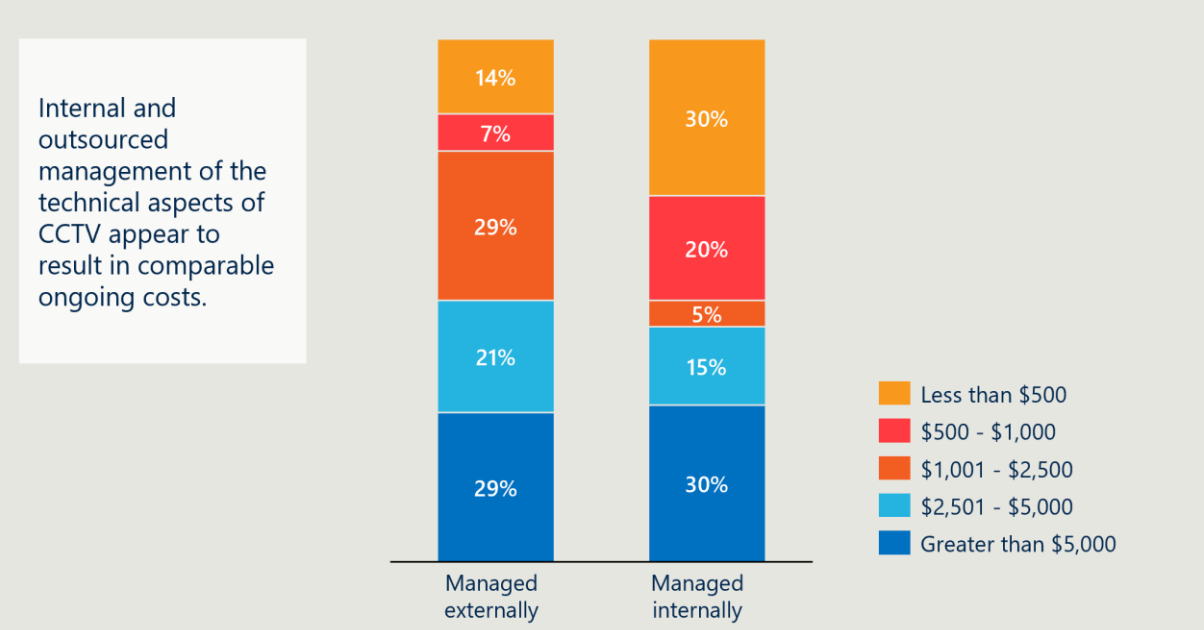
2.3.2 Operating costs for services and providers

Medium and large providers are more likely to outsource technical management of CCTV.

Unlike installation costs, ongoing CCTV costs are primarily operational expenditures, including software, maintenance, technical support and staff time. Management models vary little across the sector overall, although provider size appears to influence technical management arrangements. Small providers are somewhat more likely to manage CCTV systems internally, while medium and large providers more commonly outsource technical management to external providers.[247]

Reported annual operating costs varied substantially across providers, with no clear evidence that externally managed systems are consistently more or less expensive than internally managed systems. The most common operating cost bands were less than $500 per year and more than $5,000 per year, highlighting the significant variation in ongoing expenditure.[248]

Figure 11 | Distribution of total ongoing annual CCTV costs by management model among providers participating in the Assessment



Source: Service/Centre Manager Survey 1, and Head Office Survey

Variation in operating costs is evident across both on-premises and cloud storage models, as well as among AI-enabled and non-AI providers, with annual costs ranging from under $500 to more than $5,000 across all groups. No clear relationship was observed between ongoing costs and either storage approach or AI capability, suggesting there is insufficient evidence to explain the variation in operating costs using these factors.[249]

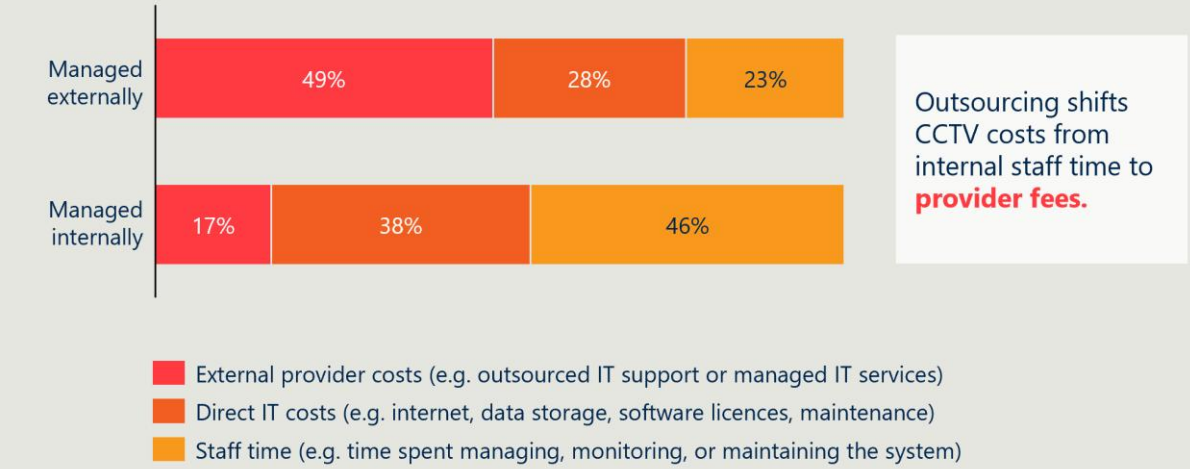
[246] Surveillant, Cloud Video Surveillance Pricing: 2026 VSaaS Cost Guide, (accessed 25 July 2026), https://surveillant.ai/guides/cloud-video-surveillance-pricing.
[247] Service / Centre Manager Survey 1, Head Office Survey
[248] Ibid
[249] Ibid

By comparison, installation costs are strongly associated with ongoing expenditure. Providers that spent more than $10,000 on installation accounted for around 90 per cent of those reporting annual operating costs above $5,000, while all providers that spent less than $2,500 on installation reported annual operating costs of $1,000 or less.[250] This suggests that system scale and complexity drive both upfront and ongoing costs, with larger and more sophisticated CCTV systems creating a sustained operating cost burden through higher maintenance, storage, technical support and management requirements.

Outsourcing shifts CCTV costs towards third-party provider fees.

Among providers that outsource technical management, external third-party provider fees account for approximately half of ongoing CCTV expenditure, making them the single largest operating cost category. Outsourcing does not appear to substantively affect overall operating costs, but it changes who bears those costs. Externally managed systems convert internal staff effort into predictable provider fees, while internally managed systems rely on service leaders and staff absorbing that effort themselves.[251]

Figure 12 | Outsourcing shifts CCTV costs from internal staff time to provider fees



Source: Service/Centre Manager Survey 1, and Head Office Survey

This suggests that decisions about CCTV management are less about reducing operating costs and more about where those costs sit within the organisation. While outsourced models make ongoing costs more visible through vendor invoices and service contracts, internally managed systems may rely on staff time that is not always tracked or attributed directly to CCTV operations.

2.3.3 Costs for regulatory authorities

Regulators have limited visibility of the costs associated with their use of CCTV.

CCTV-related activities are embedded across existing regulatory, investigative and administrative functions, rather than being recorded as a discrete area of work. As a result, RAs were generally unable to estimate the annual costs incurred by them associated with CCTV-related technology, data storage systems, software licensing or workforce effort. Authorised Officers and investigators do not typically record time spent on CCTV-related activities separately from their broader responsibilities, making it difficult to quantify the resources devoted to reviewing, managing and using footage across the regulatory process.[252]

[250] Service / Centre Manager Survey 1, Head Office Survey
[251] Ibid
[252] RA data

Further, there is no central record on the extent to which CCTV footage is available or used, making it difficult to produce national analysis on the net costs of CCTV from a RA perspective.[253]

However, there is measurable staff effort related to the use of CCTV.

RAs advised that reviewing and interpreting footage requires substantial staff time. CCTV work extends well beyond the initial viewing of footage and can involve repeated analysis, collaboration between Authorised Officers, investigators, Team Leaders and senior assessment staff, technical support to services, and additional review when matters are escalated for investigation.[254]

Where RAs were able to estimate workforce effort, footage review accounted for the largest share of CCTV-related activity, closely followed by documentation and case management. These responsibilities were generally shared across compliance, assessment and investigation. Only two jurisdictions were able to estimate the total workforce effort dedicated to CCTV-related regulatory activity – one estimating 1.55 FTE and another estimating 2.24 FTE across these functions.[255]

Importantly, the resource burden is not limited to frontline regulatory staff. Administrative teams often undertake significant work to coordinate the receipt of footage, manage secure sharing arrangements, distribute links through SharePoint-based systems, and respond to service queries. In addition, in some cases, there was significant time involved to obtain the footage in the first instance.[256] In one example, we heard that a regulator drove for an hour in both directions to collect a USB memory stick with downloaded CCTV footage to view.[257]

Further, despite RAs providing guidance materials, services frequently require step-by-step assistance to upload evidence (with RAs not necessarily being in a position to provide comprehensive advice). In these and related cases where services have limited understanding of how footage should be captured, stored or transferred, this creates additional workload for the RA (as well as the service).[258] Such reported experiences highlight the importance of clear guidance on the transfer and management of CCTV footage.

The lack of robust data on resource implications of CCTV use makes it difficult to forecast the impact of its further penetration across the sector. RAs did anticipate, however, that wider adoption of CCTV would likely require additional capability and capacity to manage footage across its lifecycle. This includes receiving, storing and reviewing footage, managing access and retention requirements, facilitating redaction, maintaining cybersecurity and audit controls, and providing legal, privacy and technical support. [259]

While CCTV generates some efficiencies by reducing the need for, or length of witness testimonies, and facilitating a clear resolution of investigations, it remains unclear whether these benefits fully offset the costs involved. As noted earlier, there were differing views on this: in most cases, RAs did not see CCTV as delivering efficiencies, but in one the estimate was that it reduced the time involved in investigations by 20-30 per cent.[260]

[253] RA data
[254] Ibid
[255] Ibid
[256] Ibid
[257] RA interview
[258] Ibid
[259] RA data
[260] RA interview

3 Key findings and implications for future policy considerations

3.1 Conclusions

The Assessment gathered data through a range of mechanisms to understand current practice and explore different use cases for CCTV, with a view to weighing the overall benefits, costs, limitations and risks. An overview of findings are included below, before listing those regarded as most important to guide future policy considerations.

Benefits

It is clear that the predominant value of CCTV is its ability to provide, in some but not all circumstances, a definitive view on what transpired before, during and after an incident affecting child safety. Regulators greatly appreciate the option of consulting CCTV footage in their investigations, stating that it expedited their resolution (with one regulator estimating that it could reduce the time involved by as much as 20-30 per cent). Services similarly value CCTV for clarifying the circumstances surrounding an incident, and staff consulted for the Assessment expressed very strong support for CCTV due to its potential to protect them from unsubstantiated allegations.

Of interest was the small but significant number of services who saw an additional benefit in the use of CCTV to support improved supervision practices and broader safeguarding and quality improvement. Some providers and services participating in Scenarios that required different forms of proactive monitoring or targeted review found this to be difficult to do given workforce capacity pressures. However, others (including participants who were not part of those Scenarios) thought it valuable to purposefully review footage unrelated to following up on a complaint or incident. They found this possible to do in small periods of time, and that doing so often revealed patterns that informed changes to practice at the service. In a similar vein, there were examples where CCTV footage was used in team meetings to share learnings.

As a general point, the Assessment perceived that the more services were asked to think about their use of CCTV (i.e. regardless of which Scenario they were involved with), the more inclined they became to using it in the interests of improving both quality and safety.

From a regulatory authority perspective, several noted that they identified issues of concern as a by-product of reviewing footage related to a specific (not necessarily related) incident. One has occasionally requested footage to review practice on a normal day to see "what happens when the regulator isn't looking,[261] enabling them to identify patterns of behaviour. Similar to the benefit identified above with respect to reflective practice, another regulator commented that reviewing footage may not reveal otherwise undetected incidents, but did provide a more detailed understanding of context and practice.[262]

Costs

Installation costs are mainly driven by the price of the hardware, including the CCTV cameras and storage units, as well as the labour associated with using professional installers. The price of the cameras often depends on their resolution, form and features (e.g. whether there is embedded AI functionality). Nous' analysis of the current state found that installation costs varied from as little as $1,000 to over $70,000. Importantly, that range did not necessarily reflect the size of the service: a four-camera setup was observed in a service with some 80 children, and a 61-camera setup for one with 120.

[261] Interview with a regulatory authority, July 2026
[262] Interview with a regulatory authority, July 2026

There is often a trade-off between upfront and ongoing costs. Physical storage options (e.g. DVRs and NVRs) can carry significant upfront hardware and installation costs but often carry minimal ongoing costs, except for occasional maintenance. Conversely, cloud storage services have lower upfront costs but carry ongoing subscriptions to store footage. For example, it can cost over $2,000 to install 12TB of physical hard drive storage, while a subscription for cloud storage can cost $180 a month.

In general, those services that incurred significant upfront installation costs (over $10,000) were more likely to incur high annual operating costs (over $5,000). This suggests that system scale and complexity drive both upfront and ongoing costs, with larger and more sophisticated CCTV systems creating a sustained operating cost burden through higher maintenance, storage, technical support and management requirements.

Some services use third parties to manage the installation, maintain the equipment and store the data, while others take more of a 'DIY' approach. Outsourcing does not appear to substantively affect overall operating costs, but it changes who bears those costs. Externally managed systems convert internal staff effort into predictable provider fees, while internally managed systems rely on service leaders and staff absorbing that effort themselves. Most services were keen to have access to more information to inform their procurement decisions.

Limitations

There are clear limitations on the efficacy of CCTV for the purposes of strengthening child safety:

1. **There are restrictions - appropriately so - on camera placement**. CCTV may have limited effectiveness as a tool for preventing sexual harm in ECEC settings, given cameras are not permitted in private areas, which expert stakeholders identified as the locations most commonly associated with offending. Across the Assessment, it was most valuable with respect to investigation of physical injuries. The few reported examples related to 'neglect' covered both detection and reflection: CCTV was used to detect situations where there was insufficient supervision, and often arose in the context of reviewing footage to see if sleep checks were being done or looking at periods or areas of relatively high accidents to inform changes to supervision rosters.
2. **CCTV has limited value in detection of incidents that would otherwise be reported through other means.** 80 per cent of the 3,386 incidents recorded by Tier 2 participating services were detected through staff observation and 16 per cent through disclosure by children. Only three per cent were identified through CCTV live monitoring or retrospective review, indicating that most incidents came to light through people witnessing or reporting them.
3. **AI technology has limitations**. While AI is advancing rapidly, and use cases are emerging where the number of 'false positives' is becoming more manageable, current technology appears to limited in its value in being able to detect more acute forms of child safety incidents and risks, such as those of a sexual nature. Absent substantive AI development and changes to regulation that relate to facial recognition and camera placement, it appears unlikely that AI can become effective in detecting inappropriate adult-to-child behaviour of a sexual nature.

Risks

There are a range of risks related to CCTV use that the Assessment was aware of and sought to explore through the analysis of current sector usage. Foremost among these was the extent to which privacy was being protected and data managed appropriately. The Assessment found that there were varying levels of understanding among participating services about privacy obligations, which is not to say that they did not appreciate its importance. Most did, were eager to comply, and were knowledgeable about fundamental rules such as not placing cameras in private areas and making explicit that CCTV was being used. There was, however, circumstances where services were unclear in what was specifically required of them, particularly in relation to the retention and safe sharing of data containing images of children. As CCTV systems become more sophisticated and increasingly cloud-based and AI-enabled, the importance of robust policies and effective governance is likely to increase.

Another key risk is that CCTV could be seen by some as a potential means for reducing active supervision by ECEC staff, rather than viewing it as one of many measures to ensure a safe environment for children. The Assessment was careful to avoid creating that impression or lending any support to such views. None of the services participating in the Assessment provided any indication that they saw CCTV as a means to reduce active staff supervision, however. On the contrary, most were at pains to emphasise that effective supervision of children by trained and responsible service staff remained paramount in the defence against risks of harm. That said, the Assessment acknowledges that the sample was relatively small given the total size of the sector, and that it was skewed towards smaller services and providers.

Two other risks are evident but were not able to be considered fully in the Assessment:

1. **The effect on children of being under surveillance.** As noted in the Literature Review, which informed the Assessment's design, there is little evidence on how this, with most available research relating to older children in school environments. This likely reflects the ethical and practical challenges in directly engaging infants and young children, the need to avoid creating an 'observation effect' whereby the subjects of the study become more aware of the cameras than they otherwise might have been, and the desirability for longitudinal results to track effects over time. Overcoming these challenges was beyond the scope of the Assessment, but the issues of children's rights and the imperative to minimise negative side-effects of CCTV, suggest this is an area where more research may be warranted.
2. **Negative workplace relations impacts.** While the Assessment generally found strongly positive staff attitudes towards CCTV, some participants raised concerns about the potential for CCTV to be used in ways that extend beyond child safety purposes. The *Literature Review* for the Assessment identified risks associated with surveillance being perceived as a tool for overbearing performance management, for example. Such concerns were raised in a Community of Practice session, where a participant cautioned against use of CCTV to 'micro-manage' staff, and during site visits, where staff referred to past experiences in other ECEC services which had managers who actively critiqued staff member practices while monitoring them via CCTV. Interestingly, the Assessment also learned of managers who checked CCTV to validate or otherwise staff members' claims of workforce injury. These examples underpin the point that CCTV is best implemented in a workplace context where there are leaders who can promote a positive, child-centric culture where the focus is on continuous learning and improvement by all.

The following draws out key findings more explicitly to provide a foundation for the subsequent list of potential policy considerations for governments.

3.2 List of key findings

Key Finding 1

CCTV is a valuable tool, but there is no strong basis for a mandatory requirement to have it installed in all ECEC settings. CCTV is becoming increasingly common across the sector, driven by evolving family expectations, growing staff support for its role in providing objective evidence, and increasing interest from ECEC providers as part of a broader safeguarding strategy. Despite this, there is little support from any stakeholder group for a universal mandate. Most considered CCTV's value to depend on service context (including cultural or historical sensitivities about being surveilled) and risk profile. They also emphasised that it should complement rather than replace other safeguarding practices.

While CCTV can assist in identifying and reviewing risks, issues and incidents, there is limited evidence that its presence materially increases the detection of significant child safety incidents beyond existing safeguarding measures. Nevertheless, the Assessment acknowledges that mandatory installation can have merit in a narrow set of circumstances related to higher-risk services, both to support stronger safety cultures and provide an objective evidentiary basis for regulatory investigations and oversight. Indeed, RAs are already invoking their powers to require CCTV use with respect to some identified high-risk providers. The outcomes of NSW's

upcoming trial will likely provide governments with further evidence on the effects of mandatory installation and use of CCTV.

Key Finding 2

CCTV can contribute to child safety, but its value is highly dependent on the type of harm concerned and whether the goal is prevention, detection or response. CCTV's strongest contribution is not as a universal prevention tool, but in strengthening investigations, supporting more defensible decisions, and helping services understand how risks arise. The nature and extent of this contribution varies across different types of harm:

- **Sexual abuse –** CCTV should not be considered a primary safeguard against sexual abuse in ECEC settings. Expert advice suggests determined perpetrators are unlikely to be reliably deterred by cameras alone, and camera placement restrictions limit CCTV's ability to observe many settings where abuse may occur. That said, CCTV may nevertheless assist in identifying or verifying behaviours that precede or sit below the threshold of more serious abuse, including inappropriate conduct, professional-boundary concerns or grooming-related behaviours that may otherwise go unnoticed or unreported.
- **Physical abuse –** CCTV provides its clearest and most direct child safety benefit where physical harm or inappropriate physical conduct is recorded. In these matters, footage can improve investigative certainty, support more timely and defensible action, and help identify patterns of unsafe interactions that may otherwise rely on contested recollections or incomplete accounts. It can also support preventative action by helping services identify recurring patterns in when, where and how physical incidents occur, enabling targeted improvements to supervision arrangements and other safeguarding practices.
- **Neglect –** CCTV can also assist in identifying supervision gaps, environmental hazards and recurring practice issues that may contribute to neglect or lower-acuity risks. Its value is strongest where footage helps services understand how and why an incident occurred, such as whether children were adequately supervised, whether staff were positioned appropriately or whether environmental risks were managed effectively. Some services also reported that AI-enabled CCTV can assist in detection and response by flagging potential risks, including perimeter breaches or unexpected behaviour during sleep periods, for staff assessment. These capabilities remain dependent on human review and should be viewed as a complement to existing safeguarding practices rather than a substitute for them.

Key Finding 3

CCTV delivers value through two distinct but complementary use cases: *event-driven review*, which supports incident detection and response, and *proactive review*, which supports prevention, organisational learning and continuous improvement.

- **Event-driven review** – CCTV contributes more to understanding incidents than to detecting them. Most incidents continue to be identified by educators and carers, families and children, with CCTV primarily used to verify facts, provide context and strengthen investigations.
- **Proactive review** – this appears to offer CCTV's strongest link to prevention. By purposefully reviewing footage, services can identify supervision issues, emerging risks and opportunities for practice improvement that may not be apparent through individual incidents alone. This broader view can help services understand patterns of risk, strengthen safeguards and address underlying issues before they contribute to more serious concerns. However, these benefits must be balanced against the time involved, which may rule it out as an option for services experiencing workforce or workload pressures. Risk-based monitoring approaches could help address the challenges associated with proactive review, with Assessment findings suggesting that targeted review of shorter footage segments may deliver similar benefits to reviewing longer periods of footage.



Key Finding 4

AI-enabled CCTV may improve the efficiency of footage review by services, but it heightens risks in some areas and its child safety benefits are, at this stage of development, limited to less acute types of harm. Based on the small number of services included in the Assessment currently using AI functionality in their CCTV systems, available products are most useful in identifying relevant footage, tracking movement across camera views and issuing alerts about perimeter breaches or potential unauthorised access. The broader value of AI-enabled CCTV is constrained by services who report its inability to effectively interpret interactions between children and educators, and by the number of 'false positive' alerts requiring system recalibrations. The use of AI-enabled CCTV can amplify risks related to privacy and cybersecurity, and there is a mixed level of knowledge in the sector about how to use the technology lawfully, effectively and safely. As AI-enabled surveillance technologies continue to evolve, they may also introduce new child safety risks and unintended consequences, most notably with respect to an over-reliance on automated detection.

Key Finding 5

RAs generally regard CCTV footage, where available and of suitable quality, to be a valuable additional source of evidence. Benefits are greatest in matters where relevant conduct is clearly captured on footage and where there is ambiguity or contested views on what has transpired. In such situations, CCTV can provide an objective record that strengthens findings and supports more timely investigations and regulatory action. Several RAs reported that CCTV evidence can materially influence regulatory outcomes, enabling them to proceed with prohibitions more quickly and with greater confidence, and reducing the likelihood of successful appeals through the provision of strong, less contestable evidence. However, there are often challenges in: obtaining the footage before it is deleted, physically accessing the data and/or working with low-quality images. Some RAs also suggested that they would prefer to be able to access audio, but this is not usually possible (due in part to the different prevailing legislative requirements and sector understanding of what is allowable).

Key Finding 6

Many ECEC services lack the technical capability required to ensure CCTV systems are fit for purpose. CCTV only supports child safety where systems have appropriate coverage, reliable image quality, sufficient retention periods, timely access to footage and secure storage arrangements. Poor camera placement, short

retention periods and unreliable access can substantially reduce the value of CCTV. Many participants acknowledged limited understanding of how CCTV systems should be designed, configured and operated to maximise their effectiveness.

Key Finding 7

Services would benefit from guidance on good practice in the safe and effective use of CCTV. The governance maturity required to support safe and compliant CCTV use varies considerably across the sector, and marked variations were observed in providers' privacy, cybersecurity and data management practices. While some participants demonstrated a sound based of knowledge, which was enhanced through the process of being onboarded into the Assessment, generally there was a desire for guidance on how to meet privacy and related obligations. While advice and template policies are available from third parties, there was an appetite also for guidance to support more informed purchase and installation of CCTV systems, good practice related to data retention and sharing, and the ways in which CCTV can potentially be used as a complement to other child safeguarding measures.

Key Finding 8

CCTV appears more likely to support, rather than undermine, a strong safety culture when implemented with effective leadership. The benefits and risks associated with CCTV are heavily influenced by how it is introduced, governed and used within a service. The Assessment found limited evidence that CCTV adversely affected workforce culture when implemented with clear purpose, governance and communication. Many participants described CCTV as supporting greater accountability, more confident decision-making and stronger organisational learning. Services were more likely to realise value from CCTV where leaders clearly articulated its purpose, fostered trust and transparency with staff and families, and positioned CCTV as one component of a broader safeguarding system. Effective leadership therefore plays an important role in ensuring CCTV reinforces a culture of safeguarding while maintaining the psychological safety of staff.

Key Finding 9

There are inconsistencies and areas of ambiguity across legislative and regulatory settings governing CCTV use in ECEC. The National Law and National Regulations, the main instruments regulating the ECEC sector, are largely silent on CCTV, except with respect to the requirement in the s168 of the Regulations that services have relevant policies and procedures in place. Binding rules on CCTV installation and use are mostly found in the criminal codes, surveillance, workplace and privacy legislation of States and Territories. While broadly similar in intent and coverage, the Assessment found several areas that would benefit from further clarity and improved consistency in how the laws are interpreted and applied – for example in relation to audio recording, parental access to footage and data retention periods. This would make it easier for multi-jurisdictional providers to operate with consistent policies, procedures and governance arrangements, and would improve certainty on such issues as footage sharing, retention obligations and the use of AI technologies that rely on biometric data.

Key Finding 10

The CCTV market is becoming increasingly diverse, creating both opportunities and challenges for ECEC services. Options range from simple camera installations to sophisticated systems incorporating cloud storage, advanced analytics and AI-enabled monitoring capabilities. This diversity provides great flexibility for services to select solutions suited to their context and safeguarding objectives. However, it also places greater demands on them to assess system suitability, effectiveness, and regulatory compliance, and to weigh up alternatives – a challenge compounded by the growing market and emergent technologies. It also makes services vulnerable to a reliance on third parties, including installers and suppliers of template policies, for advice on meeting regulatory requirements. Further, not all services are equally well-served, with those in regional, rural and remote areas being more likely to face higher costs. In the context of a dynamic market, many admitted they were not well-informed purchasers of CCTV technology and said they would value clearer guidance on product specifications, installation, vendor due diligence and data management.

3.3 Future considerations for officials

The Assessment findings highlight some potential areas for future consideration by **officials**:

1. **Produce nationally consistent best-practice guidance and implementation resources for the sector**, including:
    - Key messages re-affirming that CCTV is one component of a broader child safeguarding system, rather than a standalone safeguard.
    - Guidance on CCTV camera specifications and installation (taking into account the different operating context of services); data retention; communication with families and staff about CCTV use and expectations; and measures to maximise effective use of CCTV footage, including through event-driven review and targeted retrospective review.
    - Guidance on privacy, consent, cybersecurity and footage review governance arrangements and protocols.
    - Practical implementation resources, including model policies and procedures, consent forms, privacy notices, vendor due diligence checklists, cybersecurity controls and self-assessment tools to help providers assess the maturity of their CCTV arrangements.
2. **Undertake additional consultation with First Nations stakeholders to ensure nationally consistent best-practice guidance appropriately reflects First Nations perspectives and considerations.** This could include culturally safe approaches to consultation and communication for services looking to install CCTV; the unique considerations of ACCOs and services supporting First Nations children when using or considering the use of CCTV; and the implications of Indigenous Data Sovereignty principles for the appropriate collection, storage, access, and use of CCTV footage.
3. **Develop nationally consistent views, to the extent possible,** on:
    - Expectations for obtaining, storing and sharing CCTV footage, including evidentiary standards, appropriate retention periods, footage quality and access arrangements.
    - Greater consistency, where appropriate, in legislative requirements affecting CCTV use, including questions such as whether audio should be captured, circumstances in which footage can be shared (including to parents), and requirements for appropriate use of AI-enabled technologies that rely on biometric data.
4. **Support the sector to assess the safety, effectiveness and compliance of AI-enabled CCTV technologies.** This could include appraisal of emerging AI-enabled systems, development of criteria for assessing safety and effectiveness, and consideration of issues such as false positives, privacy impacts, biometric processing, cybersecurity, vendor assurance and appropriate human oversight.
5. **Monitor the uptake of CCTV in the sector in the next two years and evaluate** whether there is a discernible correlation in services' ability to 'self-regulate and/or the emergence of unforeseen consequences (e.g. including with respect to supervision practices, a dramatic rise in costs and/or any emerging evidence about the effects of surveillance on young children). Include in this evaluation an update on the development and deployment of AI technology as part of CCTV-based monitoring.

OPTIONAL: Subject to the outcomes of the NSW trial, consider whether targeted CCTV installation requirements may provide an appropriate complement to existing regulatory approaches for services with significant quality or safety concerns.

3.4 Future considerations for the sector

ECEC sector peak bodies and providers already play an important role in child safety and have responsibilities for the safe management of CCTV systems. Observations from the Assessment identified opportunities to

further strengthen capability, promote best-practice, and support the safe and effective use of CCTV across the sector. These actions could complement any future actions taken by governments, recognising that maximising the value of CCTV requires coordinated action across the ECEC ecosystem.

To maximise the value of CCTV, **sector peak bodies** could:

1. **Promote awareness of the proposed best-practice guidelines to build capability and understanding regarding the effective, ethical and appropriate use of CCTV.** This could include sharing examples of 'dos and don'ts' and effective use of CCTV for reflective practice. In so doing, emphasise the importance of context and consent, noting that it may not be appropriate or feasible for some services to use CCTV.
2. **Support peer learning and the sharing of good practice across the sector.** This could build on the Communities of Practice established through the Assessment and include mechanisms for providers to share lessons regarding effective use of CCTV and the safe adoption of emerging AI technologies.
3. **Incorporate references to CCTV and its appropriate use into broader capability development and leadership training initiatives.** This could reinforce the importance of positioning CCTV within a broader culture of child safeguarding strategies, risk awareness and continuous improvement to reinforce messages from government best-practice guidance.

Individual providers could also:

1. **Undertake appropriate due diligence when procuring CCTV and AI-enabled technologies.** This includes understanding how information is collected, stored, processed and protected; how vendor systems operate; and whether AI-enabled capabilities are safe, effective and appropriate for use in ECEC settings.
2. **Model appropriate leadership and maintenance of a workplace culture that supports the appropriate use of CCTV** and acts, to the extent possible, in line with the proposed best-practice guidance.
3. **Incorporate into communications with the workforce and families the provider's view on CCTV's role and value**, including to underline its limitations. This should include clear information regarding how footage is used, who can access it, how it supports safeguarding, and what it cannot reasonably be expected to do.
4. **Use CCTV to support organisational learning and continuous improvement.** In addition to supporting investigations, providers should consider how footage can be used to identify patterns of risk, inform supervision practices, improve environmental design and strengthen broader safeguarding arrangements.
5. **Periodically review the effectiveness, impacts and governance of CCTV systems.** This could include consideration of staff and family feedback, system performance, emerging privacy or cybersecurity risks, and whether CCTV is delivering the intended safeguarding outcomes. It can also help identify any emerging issues with respect to inappropriate or ineffectual use of CCTV.

Appendix A Outcomes framework

	Outcomes	Indicators	Data Sources			
			Surveys	Focus Groups	Fortnightly monitorin	Evaluative analysis
DETECTION	**Risks and incidents are identified in a more timely and comprehensive way**	Proportion of issues and incidents for which CCTV footage was fully or partially usable, grouped by type of harm	✓	X	✓	X
		Proportion of incidents detected through risk-based monitoring vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Proportion of issues / risks identified through risk-based monitoring vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Proportion of incidents detected in risk-based review vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Proportion of issues / risks detected in risk-based review vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Proportion of incidents detected in random review vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Proportion of issues / risks detected in random review vs proportion detected in event-driven scenarios (BAU)	X	X	✓	X
		Number of true positive alerts to child safety risks or incidents detected through AI-enabled monitoring, compared to BAU.	✓	X	✓	X
		Staff and providers feel that the use of CCTV has supported the identification of issues / risks	✓	✓	X	X
		Staff and providers feel that the use of CCTV has supported the identification of incidents	✓	✓	X	X
	Staff are more alert to safety risks and inclined to act on them.	Trend in the number of reports of safety issues, risks and incidents by staff over the course of the Assessment, grouped by type of harm	✓	X	✓	X

Outcomes		Indicators	Data Sources			
			Surveys	Focus Groups	Fortnightly monitorin	Evaluative analysis
		Staff operate on the basis that incidents of harm will be recorded on CCTV and detected by the service manager or regulator	✓	✓	X	X
		Staff self-assessment of whether they felt a stronger inclination during the Assessment to identify and respond to safety risks / issues due to increased awareness of CCTV and how it was being used	✓	✓	X	X
	Children or families are more likely to report incidents promptly	Parents' perception that corroborating evidence increases their likelihood of making reports	✓	X	X	X
	Improved knowledge of what best practice camera placement looks like in different services based on size, location (e.g. within an office building or standalone) and configuration	Extent to which CCTV minimises blind spots	✓	X	✓	X
		Extent to which issues/risks or incidents are detected by cameras placed in non-standard areas (i.e. all areas other than the main room/s or outdoor areas)	X	X	✓	X
RESPONSE	Staff expect that responses to reported issues and incidents will be less equivocal and more timely (than would be the case without CCTV corroboration).	Staff / provider perception that there is reduced time between incidents and action as a result of CCTV, and responses to issues are less ambiguous	✓	✓	X	X
		Proportion of investigations that produce a definitive outcome for services in the Assessment vs. a comparable sample of investigations where CCTV was not installed	✓	X	✓	✓
		Average time taken for investigations to produce a definitive outcome for services in the Assessment vs average time taken for a comparable sample of investigations where CCTV was not installed	✓	X	✓	✓
		Average staff resources required for investigations to produce a definitive outcome for services in the Assessment vs average staff resources for a comparable sample of investigations where there was not CCTV installed	✓	X	✓	✓
	Regulators and providers use CCTV footage widely	Per cent of incidents where footage was used to support an investigation, grouped by type of harm	✓	✓	✓	X

	Outcomes	Indicators	Data Sources			
			Surveys	Focus Groups	Fortnightly monitorin	Evaluative analysis
	to inform incident investigation and facilitate their fair resolution	Per cent of risks, issues and incidents where footage was used to support an investigation, grouped by type of harm	✓	✓	✓	X
	Improved understanding of appropriate retention periods.	Per cent of complaints that occur after the retention period has ended	✓	X	✓	X
	For acts of harm concealed by blind spots, or abusive behaviours undetectable by CCTV, CCTV footage provides corroborative contextual or circumstantial evidence	Per cent of cases where footage provides corroborative contextual evidence for concealed acts of harm	X	X	✓	X
	Improved understanding of current access, privacy and consent protocols in place across the ECEC sector.	Proportion of services seeking to participate that have policies in place (data source: Nous' EOI process)	X	X	X	✓
		Overall quality of the privacy, consent and data management policies provided	X	X	X	✓
PREVENTION	**Insights support continuous improvement to safety protocols, CCTV use and, where appropriate, relevant legislation.**	Number of improvement actions implemented based on insights from footage	✓	✓	✓	X
		Per cent of services who updated their protocols on the use of CCTV over the course of the Assessment	✓	✓	✓	X
	Providers, services and regulators have a better understanding of times and places of highest risk.	Most frequent times and locations occurring in incident reports, grouped by type of harm	✓	✓	✓	X
	Staff work together to support a more safety-aware workplace, and there are no negative impacts on morale or perverse incentives to 'hide' behaviour.	Positive shift in safety-related workforce survey responses over the course of the Assessment	✓	✓	X	X
CONFIDENCE IN THE SECTOR' S USE OF CCTV	**Families and staff have greater understanding and confidence in the purpose and use of CCTV in their child's ECEC service.**	Shift in parent and staff understanding and confidence in the purpose and use of CCTV for child safety in ECEC settings	✓	✓	x	x
	Risks introduced by CCTV are minimised (e.g. anxiety or	Change in the percentage of providers that experience incidents regarding cybersecurity; privacy	✓	✓	✓	x

	Outcomes	Indicators	Data Sources			
			Surveys	Focus Groups	Fortnightly monitorin	Evaluative analysis
	trauma on the part of First Nations people associated with surveillance; creating a data 'honey pot').	or data capture, storage, access, sharing and destruction in the context of CCTV use				
		Children's perspectives (conveyed via parents/carers) on the presence of CCTV cameras	x	✓	x	x
	Experts and sector representatives understand the impact, if any, of CCTV on practice	Perceptions of staff on the impact of CCTV on their interactions with or supervision of children	✓	✓	x	x
	The Assessment identifies best practice in communication with families, and engagement with First Nations representatives on specific cultural protocols that ought to be respected.	Perceptions of families on how well they were communicated to about the use of CCTV in their child's service	✓	✓	x	x
EVIDENCE TO INFORM POLICY MAKING	**Governments have access to a strong evidence base to inform advice on 'best practice' use of CCTV surveillance, including with respect to different service types and delivery contexts.**	Evidence base includes sufficient data across the five variables for which the Assessment is seeking proportionate representation: jurisdictional representation, provider size, service type, ownership structure and geographic location	✓	✓	✓	✓
		Representation of stakeholder types in the demographics of survey respondents	✓	✓	x	x
	Experts and sector representatives have visibility of Assessment findings that can inform consideration of the risks, benefits, costs and disbenefits of using CCTV in ECEC and similar settings.	Key findings from the Assessment are made available to experts and sector representatives	✓	✓	✓	✓
	Governments and the sector have an understanding of different resourcing costs vs benefits of more proactive monitoring models and whether risk-based review of footage is more effective than random sampling.	Resourcing impost of different monitoring models	✓	✓	✓	x
		Costs associated with equipment, storage locations (e.g. on premises, off premises and cloud-based), maintenance, licensing fees etc.	✓	✓	x	x
		Differences in outcomes from risk-based vs random sampling of footage	✓	✓	✓	x
	The Assessment provides evidence for whether regulatory requirements related to the safe use of CCTV need to	Number and types of issues identified through services' reporting that reveal ambiguity, gaps or other weaknesses	✓	✓	✓	x

Outcomes	Indicators	Data Sources			
		Surveys	Focus Groups	Fortnightly monitorin	Evaluative analysis
be strengthened or made more consistent.					
The Assessment provides evidence for whether a targeted mandatory requirement for high-risk providers to use CCTV delivers a marked change in culture and/or safety outcomes	Staff perspectives on the use of CCTV vary between scenarios where it is voluntary or imposed	✓	✓	x	x
	Number of incidents compared across scenarios	x	x	✓	x

Appendix B Site visit case studies

CASE STUDY 1

SOPHISTICATED (NON-AI) CCTV SYSTEM



SERVICE CHARACTERISTICS

Long day care | Privately owned | Regional | 106 Approved places

CONTEXT

Some providers have invested in advanced CCTV systems and associated technology, which provided comprehensive coverage. This case study is based on one such example.

BACKGROUND

The service has operated for over a decade and is one of three owned by a small multi-site provider. CCTV was put in place from the outset. The owners bring experience in information technology, which directly shaped how the CCTV system was designed and managed. They also use facial recognition software to control access which in turn links to their time and attendance platform for staff.

PROCUREMENT

The owners' comfort with technology means that they have not needed to rely on external advice but could undertake their own research on the purchase of CCTV equipment. This included attending an industry convention where security systems were showcased. The overall cost for CCTV installation in the site visited was $65,000 - $70,000. In addition, the service used their subscription to a business advisory platform to access and tailor appropriate CCTV-related polices for their services.

SET UP

The site visited has 106 enrolled children and has 61 cameras across internal and external area. It includes all enclosed spaces, including storerooms, other than staff rooms and toilets. There are only two blind spots, both in the outdoor area. The owner would ideally like to install a 360-degree camera on a pole to remove these, but this would be logistically difficult and expensive.

There are two large monitors in the managers' office, one each for the indoor and outdoor cameras. They are both motion-sensitive – highlighting fast movements of children and adults – and light-sensitive, so perform in low light. Resolution of cameras is high, so even though the large monitor is a split screen with feeds from most of the 61 cameras, visibility of activity across the service is very high. External cameras can read number plates.

GOVERNANCE AND DATA MANAGEMENT

ACCESS

CCTV footage is stored onsite and held for a two-week cycle. Access is restricted to managers, with staff requiring prior approval before recordings are viewed. The service maintains strict policies around the sharing of footage. For example, staff require prior approval from one of the owners to review footage, and one owner must be present when reviewing.

When owners have had to share footage with the regulator they have done so through a removable memory (USB) stick form which they pick up from the service.

Families at the service had not raised concerns about the presence of CCTV. On the contrary, CCTV had become a significant factor in enrolment decisions, with prospective families informed of it upfront. The service was the only one in its area with cameras in place, and the owners reported that CCTV had become a fundamental consideration for families choosing where to enrol their child.

CASE STUDY 1

SOPHISTICATED (NON-AI) CCTV SYSTEM

HOW THEY USE CCTV

MONITORING APPROACH

Owners described their approach to monitoring as incidental and event-triggered rather than scheduled. This was a conscious choice framed around avoiding a 'big brother' culture in the service.
That said, there was at least one instance where management used CCTV footage to investigate whether a staff member was making a legitimate workcover claim (that related to lifting a heavy object).

PRIMARY VALUE

The owners saw CCTV being of most value in the following circumstances:

- **Responding** to parent concerns including to support regulatory investigations
- **Investigating** child safety incidents and near misses
- **Providing** evidence for inquiries into theft or damage to property

Footage is also occasionally used as a staff training resource, where recordings are used to inform or reinforce messaging about child safety and good practice in education and care.

In a small number of cases, AI number plate interpretation was used to identify restricted individuals attempting to pick up children from the service by alerting management.

Overall, the owners likened CCTV to speed limits and cameras, seeing CCTV as an effective deterrent to illegal behaviour and an incentive to follow good practice. The owners therefore advocated for CCTV to be mandated across all ECEC services. They saw it as a standard inclusion increasingly being considered standard and noted that it would be inequitable for some children to not have the same level of protection that CCTV can provide.

STAFF AND FAMILY VIEWS

STAFF

Staff are informed of CCTV at onboarding. They are used to CCTV and have no objections, partly because they are aware that the intent is to identify issues and risks relating to child safety and not to monitor performance.
An individual staff member interviewed said she valued the role of CCTV in settling disputes or responding to allegations. The educator described an instance where a child's allegation of being hit was investigated through footage, which confirmed the contact has been incidental, protecting an educator from adverse consequences.
As a safety tool, footage enabled the identification of near misses that might otherwise have gone unnoticed and informed how children were positioned within activity areas to maintain optimal camera coverage. The same educator raised a concern about the quality of incoming staff, observing a decline in competency over nearly four decades in the sector and attributing this in part to fast-tracked qualifications, a concern that situated the protective and developmental value of CCTV within a context where foundational workforce quality can no longer be assumed.



FAMILIES

Staff at the service noted that parents now hold higher expectations of services, and access to CCTV provides important reassurance.

CASE STUDY 2

BASIC CCTV SYSTEM AND COVERAGE



SERVICE CHARACTERISTICS

Long day care | Privately owned | Regional | 49 Approved places

CONTEXT

Some services operate quite limited CCTV systems that provide basic coverage. This case study is based on one such example.

BACKGROUND

This service opened two years ago and is attached to a primary and high school, with CCTV being in place since the construction of the Early Learning Centre. The CCTV is an extension of the school's system and is managed centrally by the IT department. The school is in an area where property crime, vandalism and drug-related incidents are known local risks.

PROCUREMENT

The service drew on the school's existing supplier and IT team. Cameras were selected to match those already in use across the broader campus. Installation was conducted by an IT staff member who was also a qualified electrician removing the need for an external vendor. The service used their subscription to a business advisory platform to access and tailor appropriate CCTV-related polices for their service.

SET UP

The service has 13 cameras all externally positioned. Cameras cover the building perimeter, entrances and the outdoor play yard. No cameras are inside the service. The cameras are small and mounted under the services veranda. There is one significant blind spot at a cubby house at the far end of the shared outdoor play yard. Their service has expressed interest in installing cameras inside the centre, but no decision has been made with the campus principal with budget constraints and uncertainty about indoor regulatory requirements identified as barriers.

Footage is stored off-site on the school campus IT infrastructure, with no monitoring capability located at the service. Recordings are manually deleted after a four-month cycle.

GOVERNANCE AND DATA MANAGEMENT

ACCESS

There are no monitors at the service. Footage is accessed through the school's IT team, who will retrieve and review the relevant recordings and present them to the service manager.

There is no established protocol for sharing footage with the regulator, as this situation is yet to occur.

In a few cases, footage was requested by and provided to police, in connection with a property damage incident.

Families receive a letter advising of the presence of CCTV at the service. To date these have prompted only two responses, both positive.

Footage is not made available to parents to view.

CASE STUDY 2

BASIC CCTV SYSTEM AND COVERAGE

HOW THEY USE CCTV

MONITORING APPROACH

The service does not actively monitor CCTV. Footage is accessed reactively, on an as-needed basis, through the IT team. The service saw this as a significant limitation on the extent to which they can get value from CCTV.

PRIMARY VALUE

The service director regarded CCTV to be of most value in:

- **Investigating** child safety incidents, including confirming how injuries occurred.
- **Providing evidence** in connection to property damage to service and staff property.
- **Improving parent behaviour** with respect to the leaving infants unattended in vehicles.

The service thought that, in theory, there might be value from CCTV in supporting reflective practice, but without any external cameras or ready access to footage, this was not an option. That said, CCTV has had led to some improved practices (see below).

STAFF AND FAMILY VIEWS

STAFF

CCTV was discussed at staff meetings in the context of the service's participation in the Assessment. Since then, the service manager has noticed a positive change in staff behaviour. Educators and carers were seemingly more aware of their positioning in the play areas and the need for full supervision. The manager had also detected a shift towards more measured communication with children. These changes were attributed to the discussion of potential use of CCTV for reflective practice rather than simply being re-sensitised to the presence of cameras.

One staff member interviewed had experience of CCTV being used for active performance monitoring at another service. They had instinctive reservations about the placement of cameras indoors, but said their views on this had since changed. Working occasionally alone with children – some of whom had previously caused psychical harm towards her – they felt they would now welcome internal cameras, both for the safety of staff and of children.



FAMILIES

Staff said that CCTV was not normally raised by prospective families during tours. Nor has the service received any negative feedback about the cameras.

Similarly, families' responses to participation in the Assessment were negligible.

CASE STUDY 3

CCTV AT MULTI-SITE PROVIDER WITH THREE PARTICIPATING SERVICES

PROVIDER CHARACTERISTICS				SERVICE 1	SERVICE 2	SERVICE 3
Long day care	Privately owned	Metropolitan	Medium sized	98 Approved places	100 Approved places	92 Approved places

CONTEXT

Some providers manage CCTV across multiple sites, subject to consistent governance practices while adapting to the local environment at each location. This case study is based on one such example, drawing on visits to all three services operated by the provider.

BACKGROUND

The provider operates three services in one jurisdiction, each having CCTV installed indoors and outdoors. Two of the three sites have operated for a number of years while its third site opened in 2025. Each service has a service manager and a regional manager that is involved in the day-to-day oversight of centres. The owners noted that direct, hands-on involvement is essential to managing CCTV governance effectively, and that less engaged operators would likely struggle with the operational and oversight requirements.

PROCUREMENT

The provider engaged an external technology contractor to supply, install and maintain CCTV hardware and software across all three sites, including remote access capability. Installation costs ran to five figures across the provider's services, an outlay the owners characterised as an investment and exercise in future proofing. Ongoing maintenance has cost approximately $1,000 in total across the life of the systems at each location.

SET UP

Coverage quality varies across the three sites The newest site has the strongest system, with high resolution footage. This includes low light functionality, motion-triggered event categorisation, near-live feed capability, and number plate recognition The two older sites face greater limitations due to retrofitting constraints In particular, the inability to run power to external fence lines has created blind spots around outdoor play equipment. One of these sites has more blind spots than the other two because of the team not being involved in its original construction

No cameras are installed in staff rooms, bathrooms, or toilets. Where CCTV cannot provide coverage, including laundry areas identified as higher-risk spaces, the provider has made physical design changes to reduce risk, such as installing glass doors to enable line of sight visibility.

GOVERNANCE AND DATA MANAGEMENT

ACCESS

Access to footage is restricted to management across all three sites. Parents are not given direct access to recordings. Where footage is relevant to a concern, staff review it and communicate findings to families without sharing the footage itself.

The provider has not been required to share footage with the regulator to date but could do so directly or via their technology contractor, if required.

Parents are informed of CCTV at enrolment and must formally acknowledge its presence. Signage is also displayed across all services. CCTV has become a positive consideration in enrolment decisions for many families, with prospective parents frequently raising it during orientation tours.

CASE STUDY 3

CCTV AT MULTI-SITE PROVIDER WITH THREE PARTICIPATING SERVICES

HOW THEY USE CCTV

MONITORING APPROACH

Monitoring across two sites are event-based, and one proactive.

Proactive real-time monitoring is not feasible due to limited staff capacity. The regional manager noted that meaningful proactive monitoring would require a dedicated safety officer; a role the current financial environment does not enable in their context.

The exception to this monitoring approach is at the provider's newest site, where the director reviews 15 to 20 minutes of footage per week. They described this as a valuable practice improvement tool when they are not on the floor. This was a decision made by the individual director, rather than a requirement from the provider itself.

PRIMARY VALUE

The provider identified CCTV as being most valuable for resolving parent complaints and allegations against staff, investigating child safety incidents and injuries of unknown origin, and supporting police investigations.

Footage has also been used to identify environmental hazards, including one instance where a deck area was flagged as a safety risk. It is also used to monitor conduct of external contractors such as cleaning staff. At its newest site, footage has been used to identify patterns and triggers underlying episodes of emotional dysregulation and aggression, helping staff develop more informed and responsive support strategies for individual children.

The regional manager is a strong advocate for mandatory CCTV across the sector, describing it as both a deterrent to poor conduct and an equity issue; framing it as difficult to justify why some children should have less protection than others.

STAFF AND FAMILY VIEWS

STAFF

Staff across the three sites were supportive of CCTV and generally unaware of cameras during their day-to-day work. Educators are informed of CCTV at onboarding and raised no substantive objections. Male educators, in particular, valued CCTV as a source of professional protection given the heightened scrutiny their role can attract.

Staff cited a number of instances where footage had protected their professional standing, including cases where allegations of physical contact were confirmed by footage to be incidental or unfounded, and cases involving children with challenging behaviours where an objective record was important. One educator described footage as providing an emotionless account of events — particularly valuable where verbal accounts from children, parents, and staff diverge.

Some staff raised concerns about the potential for CCTV to be used punitively. One educator had previously worked at a service where footage was used to look for problems rather than to support staff development. They emphasised that leadership capability in using footage constructively was critical. A related concern was raised about the limitations of footage itself; that it captures only a fragment of events and cannot convey the full context of an interaction.



FAMILIES

Families were broadly supportive, with CCTV frequently raised as an early question during orientation. Attitudes were not uniform across the three sites, however. At one site, parents with backgrounds in defence and national security had raised concerns about being recorded. At another, concerns had been raised about cyber security and the risk of footage being accessed by unauthorised parties. Requests for live parental access to footage had been raised historically, but were not accommodated on the basis that this would be uncomfortable for staff and raised additional privacy considerations for other children in the service.

Staff observed that trust between families and services had shifted in recent years, with one educator noting that it could no longer be assumed parents would side with the service in a dispute.

CASE STUDY 4

SOPHISTICATED AI ENABLED CCTV



Service Characteristics

Long day care	Privately owned	Rural	Small sized	132 Approved places

CONTEXT

Some providers are using CCTV with embedded AI capability in the interests of exploring how it can add further ballast to their child safeguarding measures. This case study is based on one such example.

BACKGROUND

This is a rural single site provider with a purpose-built service that aims to offer a higher-quality service than others in the locality. The owner brings a high degree of technical understanding about AI-enabled CCTV, and sees it as a key feature of the service's safety culture rather than a compliance measure. The service is managed by a team of five.

PROCUREMENT

The owner conducted independent research before procuring the CCTV system, engaging directly with vendors and evaluating options based on considerations of image resolution and AI compatibility. The cameras he purchased were seen as relatively expensive, at approximately $1,000 each.

The owner characterised the overall investment as unambiguously worthwhile, but thought that the technology he was using was not affordable for most providers. He recommended that government provide financial assistance to support broader adoption.

The owner built a bespoke Ai monitoring system using an on-site server rather than a cloud-based provider. This gave him the ability to directly calibrate the system to minimise false positives.

SET UP

The service has 45 cameras across internal and external areas with hardwired, defence-rated units, which were selected for durability in a rural environment susceptible to power outages and surges. Camera placement is treated as an ongoing process rather than a one-off installation. The owner revisits positioning regularly based on observed child behaviour, common hiding spots, and lighting conditions. He said it typically takes six to nine months of iterative adjustment before a system performs reliably.

Outdoor areas are regarded as the highest-risk zone and so have received the most attention.

AI alerts are delivered in real time to a small screen at the front desk and simultaneously to Microsoft Teams, keeping relevant staff informed without disrupting workflows. Cameras operate on a dedicated VLAN, with system logs and access controls in place. The system is not set and forget, the owner can refine calibration and adjust resolution and prompt parameters.

GOVERNANCE AND DATA MANAGEMENT

ACCESS

Access to footage is tightly controlled, with the owner retaining primary oversight. The owner was deliberate about limiting staff access to footage, noting that many owners prefer to retain this control entirely.

Families are informed of CCTV at enrolment. The owner identified the security of footage storage as an important consideration for families and flagged that maintenance providers with physical access to camera systems represent a meaningful and underappreciated security risk.

CASE STUDY 4

SOPHISTICATED AI ENABLED CCTV

HOW THEY USE CCTV

MONITORING APPROACH

The AI alert system enables a form of continuous passive monitoring that does not require staff to step away from children.

This is a material advantage over conventional CCTV in a service where ratios constrain capacity for proactive review.

In addition to relying on alerts, the owner monitors footage both in real time and retrospectively, spending time each week reviewing the environment for hazards, hiding spots, and coverage gaps.

The owner estimated that the highest volume of genuine alerts relate to accidents and children exploring, rather than staff conduct.

PRIMARY VALUE

The owner identified CCTV as most valuable for protecting the interests of himself as an employer, as well as supporting improved safeguarding of children. He saw both these roles as being central to its value of CCTV.

The owner found it useful in understanding and responding to general risks to child safety. For example, analysis of likely child movement using CCTV identified how quickly a child could reach the road from the outdoor area, prompting the installation of an additional gate to slow that path and ensure AI alerts could fire in time for staff to intervene. Similarly, CCTV informed physical modifications at the service such as furniture placement to improve sight-lines.

The owner described CCTV as actively creating an analytical mindset across the workforce, with staff increasingly attentive to hazards, blind spots, and the environmental factors that affect what cameras can and cannot see. In addition, footage is used to track patterns of conflict between children and inform behaviour improvement plans. The number plate recognition functionality supports identification of restricted individuals at the gate.

The owner was a strong advocate for mandatory CCTV, noting that every family at the service is comforted by it and that members of the broader community had specifically chosen the service because of its cameras. He was equally clear, however, that mandating CCTV without addressing cost barriers, financing constraints, and landlord restrictions would set providers up for failure.

STAFF AND FAMILY VIEWS

STAFF

Staff were aware of the CCTV system and its AI capabilities and raised no objections. The owner observed that attitudes toward CCTV among staff tend to reflect prior experience rather than, for example, age. Those employees who had been through an incident or a dispute were typically the most supportive. CCTV had reportedly reduced 'he-said-she-said' debates within the team and has encouraged staff to speak up, knowing that an objective record exists.



FAMILIES

The owner reported that families' primary concern has been to confirm that cameras are not installed in bathrooms or toilet areas, and that footage is stored securely. Once satisfied on both points, support is near-universal. Members of the broader community had reportedly sought out the service based on its CCTV. The owner noted that younger families tended to be more comfortable with cameras.

CASE STUDY 5

CCTV AS A TOOL FOR REFLECTIVE PRACTICE

SITE 1	Long day care	Not for profit	Metropolitan	98 Approved places
SITE 2	Preschool	Community-based	Rural	25 Approved places
SITE 3	Long day care	Private	Metropolitan	36 Approved places

CONTEXT

Some services have found CCTV to be a useful tool for reflective practice to improve education and care, strengthen supervision practices and inform operational policies. This case study draws on three services where CCTV has been used in this way.

BACKGROUND

Each service – two metro sites and a small rural one – introduced CCTV for safety and security reasons. Over time, they saw the potential for CCTV footage to be used for a broader range of purposes, while being conscious of the need to avoid it becoming an instrument for 'catching out' or reprimanding staff. Of note, is that participation in the Assessment appeared to raise interest in using CCTV for reflective practice.

DESIGN

As reflective practice involves reviewing CCTV footage with the intent to extract learnings to inform policies, procedures or education and care practices, it follows that there must be monitors on-site that the service manager, at minimum, can access. There must also be cameras installed inside the service, with sufficient resolution and the ability to zoom to be able to study activities and interactions.

HOW THEY USE CCTV *(cont. overleaf)*

Examples below fall into three categories: using CCTV footage to improve supervision arrangements, to develop strategies for managing particularly problematic behaviours by some children, and as a source for staff development. The first two are more common uses.

SUPERVISION PLANNING

At the first service, footage was accessed to review supervision arrangements, understand how outdoor spaces were being used, and to identify opportunities to improve the physical environment. One staff member described how reviewing footage had helped her understand how to position herself to maximise supervision coverage of children.

BEHAVIOURAL MANAGEMENT

The third service said they had found CCTV useful in analysing the circumstances leading up to challenging behaviour by one child in particular, who would become visibly distressed and aggressive. CCTV cameras were repositioned to better capture the child's interactions and movements throughout the service. Reviewing footage of the incident helped staff identify triggers that were not apparent in real time, and they used this information to develop strategies for avoiding similarly heightened situations in future.

Footage was reviewed at staff meetings, where educators discussed what they observed, reflected on alternative responses and identified opportunities to strengthen practice. In one review session, staff reflected on strategies that had supported de-escalation, including getting down to the child's level, attempting redirection and setting boundaries early, as well as actions that may have unintentionally intensified the situation. These discussions informed changes to supervision arrangements, contributed to the engagement of an occupational therapist and helped staff determine when intervention was most effective.

CASE STUDY 5

CCTV AS A TOOL FOR REFLECTIVE PRACTICE

HOW THEY USE CCTV

STAFF DEVELOPMENT

In addition to reviewing incidents involving children, footage at the third service was occasionally reviewed to support individual staff development. In one example, a junior educator reviewed footage of her interactions with children following concerns raised by a colleague. This was the only example across the three services where CCTV was used directly in discussions about individual staff practice.

STAFF AND FAMILY VIEWS

STAFF

A key risk with the use of CCTV as a tool for reflective practice is that it becomes, or is seen to be, a tool for monitoring and reprimanding staff.

A manager at the second service said she was comfortable with how CCTV was being used there, but contrasted this with her experience with a previous employer, where CCTV monitoring felt more like "a performance review". In that service, directors regularly monitored live footage and contacted staff to 'correct' them while doing so. She attributed the difference to organisational culture: whereas the practice in her previous service created discomfort and distrust; in her current service, their approach made it clear that the goal was to support educators and carers to improve professional practice, in the interests of a better experience and outcomes for children.

This view was consistent with feedback provided at the other services, where staff acceptance was strong where CCTV was promoted as a tool for learning, reflection and improvement, rather than surveillance.



FAMILIES

One service used footage they had drawn on for reflective practice in their engagement with families. It was used to demonstrate to parents of a child with challenging behaviours what they had observed about certain triggers, and how the strategies developed at the service might be helpful also in the home and service setting.

Appendix C Additional CCTV market analysis

The CCTV market is well established and growing, dominated by a few suppliers

The estimated value of the Australian CCTV market is $0.9-$2.2 billion.[263] It comprises several types of market players, including manufacturers, distributors, installers and video monitoring service providers. The market is expected to grow rapidly, with estimates ranging from five to 18 per cent over the next five to 10 years.[264] This growth is mostly driven by government investment in security and critical infrastructure projects, residential security systems and the ongoing need for system upgrades and equipment replacement.[265]

The supply of CCTV cameras is led by international manufacturers, with imported equipment accounting for over 90 per cent of total equipment sales.[266] In 2021, the two largest global brands, Hikvision and Dahua, were responsible for over 60,000 surveillance networks across Australia.[267] This is reflected in the suppliers reported by participating Tier 2 services: among surveyed services who reported the manufacturer of their camera system, 57 per cent (97 services) had installed a Hikvision or Dahua branded camera or another brand that is known to use Hikvision or Dahua hardware.[268] Table 5 details the camera manufacturers used by Tier 2 services and their prevalence, segmented by country of origin. Where services used hardware manufactured by different original equipment manufacturers (OEMs), namely Swann (Raysharp), VIP Vision (Dahua) and Micron (Uniview), these were captured under the OEM.[269]

Table 5 | Camera manufacturers and usage by sampled ECEC services, by country

	China	South Korea	United States	Australia	Japan
Total service usage count	57% (97 services)	18% (31 services)	14% (23 services)	9% (15 services)	2% (3 services)
Manufacturers	• Dahua (42) • Hikvision (39) • Raysharp (7) • Eufy (2) • TP-Link (2) • Reolink (2) • Uniview (2) • Tiandy (1)	• Hanwha (31)	• Ubiquiti (15) • Avigilon (2) • Google (2) • Watchguard (2) • Cisco Meraki (1) • Wyze (1)	• IVSEC (15)	• Axis (2) • Panasonic (1)

[263] IMARC Group, Australia CCTV Market Size, Share, Trends and Forecast by Type, End User, and Region, 2026-2034, 2025 (accessed 28 July 2026), https://www.imarcgroup.com/australia-cctv-market; Grand View Research, Australia Video Surveillance Market Size & Outlook, 2026 (accessed 28 July 2026), https://www.grandviewresearch.com/horizon/outlook/video-surveillance-market/australia; Expert Market Research, Australia CCTV Camera Market Size, Share, and Trends: Forecast and Growth Analysis Report (2026-2035), 20 April 2026 (accessed 28 July 2026), https://www.expertmarketresearch.com.au/reports/australia-cctv-camera-market; Research and Markets, Australia CCTV Camera Market, By Region, Competition, Forecast and Opportunities, 2019 - 2029F, October 2024 (accessed 28 July 2026), https://www.researchmarkets.com/report/australia-cctv-camera-market

[264] Ibid

[265] IMARC Group, Australia CCTV Market Size, Share, Trends and Forecast by Type, End User, and Region, 2026-2034, 2025 (accessed 28 July 2026), https://www.imarcgroup.com/australia-cctv-market; IndexBox, Australia Cctv Camera - Market Analysis, Forecast, Size, Trends and Insights, 1 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-cctv-camera-market-analysis-forecast-size-trends-and-insights/

[266] IndexBox, Australia Surveillance Camera - Market Analysis, Forecast, Size, Trends and Insights, 3 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-surveillance-camera-market-analysis-forecast-size-trends-and-insights/

[267] Ausma Bernot and Marcus Smith, Regulating Chinese-Made CCTV Cameras in Australia, 5 September 2023 (accessed 28 July 2026), https://www.internationalaffairs.org.au/australianoutlook/regulating-chinese-made-cctv-cameras-in-australia/

[268] IPVM, Hikvision OEM Directory, 19 April 2024 (accessed 28 July 2026), https://ipvm.com/reports/hikvision-oem-directory; IPVM, Dahua OEM Directory, 3 May 2024 (accessed 28 July 2026), https://ipvm.com/reports/dahua-oem

[269] IPVM, Hikvision OEM Directory, 19 April 2024 (accessed 28 July 2026), https://ipvm.com/reports/hikvision-oem-directory; IPVM, Dahua OEM Directory, 3 May 2024 (accessed 28 July 2026), https://ipvm.com/reports/dahua-oem; micron, 6MP HD IR Fixed Turret Camera, n.d. (accessed 28 July 2026), https://d347awuzx0kdse.cloudfront.net/micron/product-download/ipc6ta_brochure.pdf

Camera features and specification determine price, with premium cameras unnecessary in most circumstances.

Overall system cost is primarily determined by the features and specifications of the cameras, such as connectivity, form, movement and resolution, and the supporting storage and video access infrastructure. Among surveyed Tier 1 services, the most common number of installed cameras was eight.

Estimates place the upfront equipment cost for an adequate eight-camera system, including required physical storage and transmission cables, at $3000 to $5000.[270] Price competition between new and established brands has resulted in an estimated annual price reduction of 3-5 per cent for mid-tier cameras and 5-8 per cent for low-cost cameras.[271] However, costs may rise in the short term, due to manufacturing cost pressures driven by semiconductor shortages, and demand for AI data centres. Australian installers reported that storage hard drive prices have nearly doubled in recent years, while lead times for physical storage servers have increased to 8–12 weeks.

Table 6 details the range of features and specifications that can influence camera price and how these differ across camera price tiers.

- **Low-cost cameras** (approx. $250 or less) are targeted toward residential customers and provide limited resolution, durability and functionality. There is more variation among low-cost cameras, due to a large selection of products and manufacturers adjusting specifications to meet specific price points.
- **Mid-tier cameras** (approx. $250 to $600) are targeted to commercial customers and offer increased resolution, durability, AI capabilities and functionality.
- **Premium cameras** (approx. $600 or more) are targeted to customers needing high security or a specialised function and offer advanced movement, AI analytics and cybersecurity functions suitable to monitoring open or congested spaces.

Table 6 | Features and specifications influencing camera price, by price tier [272]

Feature/specification	Low-cost cameras	Mid-tier cameras	Premium cameras
Resolution	2MP-4MP	4MP-8MP	8MP+
Lens type	Fixed lens	Fixed or varifocal lens	Varifocal and motorised zoom lens
Night vision	Infrared (black-and-white)	Infrared and starlight technology	Colour night vision, dual-light, advanced low-light performance
AI capabilities	Motion detection, basic human detection	Human and vehicle detection, intrusion and line-crossing detection	Advanced analytics, facial recognition, licence plate recognition, behaviour analytics
PTZ capabilities	Generally unavailable	Entry-level PTZ available	Commonly available, high-speed PTZ with autonomous tracking
Field of view	Standard single-sensor view	Wider field-of-view options	Panoramic and multi-sensor options

[270] Indicative equipment cost range is for a system comprising 8 6MP IP cameras, NVR, 12TB of hard-drive storage and cabling. System specifications and pricing was informed by consultations with professional installers and a review of publicly available pricing.
[271] IndexBox, Australia Cctv Camera - Market Analysis, Forecast, Size, Trends and Insights, 1 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-cctv-camera-market-analysis-forecast-size-trends-and-insights/
[272] Variance in specifications was derived from a review of publicly available guidance and cameras models across various retail and commercial providers.

Cybersecurity features	Basic vendor security controls with limited independently demonstrated assurance	Enhanced security controls and more mature patching practices	Independent testing, security certifications and formal vulnerability management programs
Warranty and support	Typically 1-2 years	Typically 2-3 years	Typically 3-5+ years
Durability	Basic outdoor protection (typically IP66-IP67)	Outdoor protection with some vandal-resistant models available	High durability, commonly IK10 vandal resistance, extended environmental protection and specialised industrial/marine options

Table 7 details common camera features and specifications that may influence camera price but are not differentiated by price tier.

Table 7 | Features and specifications influencing camera price

Feature/specification	Influence on camera price
Connectivity	IP connectivity is now standard across low-cost, mid-tier and premium cameras. Analogue cameras also exist across all price tiers. IP cameras tend to cost more than analogue cameras with similar specifications.
Power	Power over Ethernet (PoE) is available from low-cost through to premium cameras. Battery and solar options are also available across multiple price points.
Form factor	Bullet, dome and turret cameras are offered in all price tiers. Form factor is typically driven by use case. Professional installers indicated that bullet cameras tend to command a 30-40 per cent premium over turret cameras in professional installations and are typically used in outdoor settings where more durability is required.
Audio	Audio recording can be found in low, medium and premium cameras. Two-way audio and active deterrence are increasingly common across all price tiers.

Third-party video management platforms are available to larger providers seeking advanced, centralised management of cameras across services. Physical storage systems allow basic video playback of stored footage. Many IP camera manufacturers also provide free software that supports remote viewing, playback and basic analytics for their own cameras. However, providers seeking centralised oversight of multiple services, integration with other security technologies or advanced analytics may purchase a third-party, locally housed Video Management System (VMS) platform or cloud-based Video Surveillance as a Service (VSaaS) equivalent. VMS solutions are generally purchased upfront at around $200 to $500 per camera and incur annual maintenance fees of 15–21 per cent of the initial licence cost. By contrast, VSaaS solutions are subscription-based and typically cost $10–150 per camera per month.[273] These ongoing licensing and maintenance costs can become substantial as camera numbers increase. As a result, VMS and VSaaS solutions are generally only cost-effective for larger providers operating multiple services. Only one Tier 2 service reported using a VMS provider (Genetec).

Licensed operators play a key role in compliant CCTV installation, but supply is uneven.

The licensed operator market is fragmented, varies by jurisdiction and its size is difficult to measure. IBISWorld estimates that there are approximately 1,763 security system installation and monitoring businesses across

[273] Falguni Chatterjee, VMS Pricing 2026: Per-Camera vs Flat Rate, 14 July 2026 (accessed 28 July 2026), https://visylix.com/blog/vms-pricing-comparison-2026#pricing-model-breakdown-per-camera-vs-flat-rate-vs-usage-based; TetherX, VSaas Explained, 2026 (accessed 28 July 2026), https://tetherx.io/what-is-vsaas#vsaas-pricing

Australia.[274] The Australian security industry's peak body, Australian Security Industry Association Limited (ASIAL), estimates that its 986 members represent 85 per cent of the total number of CCTV sales and installation businesses nationwide, which would suggest there are approximately 1,180 CCTV providers. [275] [276]

The CCTV services market is highly fragmented: 89 per cent of ASIAL members providing CCTV services are 'small' businesses, defined as entities that generate less than $2.5 million in annual revenue.[277] The operator market is also emerging: 19 per cent of ASIAL members providing CCTV services were established in the last six years.[278] This reflects broader national security licensing trends, with total individual and business security licences growing by 13 per cent and 18 per cent respectively from 2019 to 2024.[279]

Preliminary supplier analysis indicates that regional and remote areas are at risk of thin market conditions. The distribution and size of the licensed operator market is difficult to measure and compare across jurisdictions. In some jurisdictions, a single generic individual license applies for a range of security related services, while in other jurisdictions, employees of a licensed business may not need to hold an individual license. As a result of this disparate licensing system, it is difficult to distinguish which operators offer CCTV installation services, their market capture and place of business on the basis of licensing information alone.

However, analysis of ASIAL membership and ECEC service registration data indicates that some regional and remote areas experience a higher risk of thin market conditions. Figure 13 represents the outputs from detailed market analysis, which score each Australian postcode based on the following factors:

- **Supply:** number, location and likely delivery capacity of ASIAL registered members
- **Demand:** the number, location of ECEC services and number of approved places at each service
- **Access:** ECEC services proximity to ASIAL registered members

In postal areas shaded dark blue, ECEC services have access to a wide choice of nearby suppliers and can generate sufficient demand to drive a competitive, large supplier market. In areas shaded light blue, ECEC services rely on relatively fewer, smaller or more distant suppliers, and lower demand levels constrain suppliers from entering these 'thin market' areas. This analysis indicates that, although demand from ECEC services declines with remoteness, supplier availability and capacity declines even more rapidly:

Supply: Metropolitan postal areas have access to 149 ASIAL registered suppliers within 50 km, 4.7 times more suppliers than regional centres (32) and 50 times as many suppliers as very rural and remote areas (2.8).

Demand: Metropolitan postal areas contain 13 ECEC services on average, 1.6 times more services than regional centres (8) and more than 11 times as many services as small rural and remote areas (1). Services in rural and remote areas also have fewer approved places on average and so likely require fewer CCTV cameras.

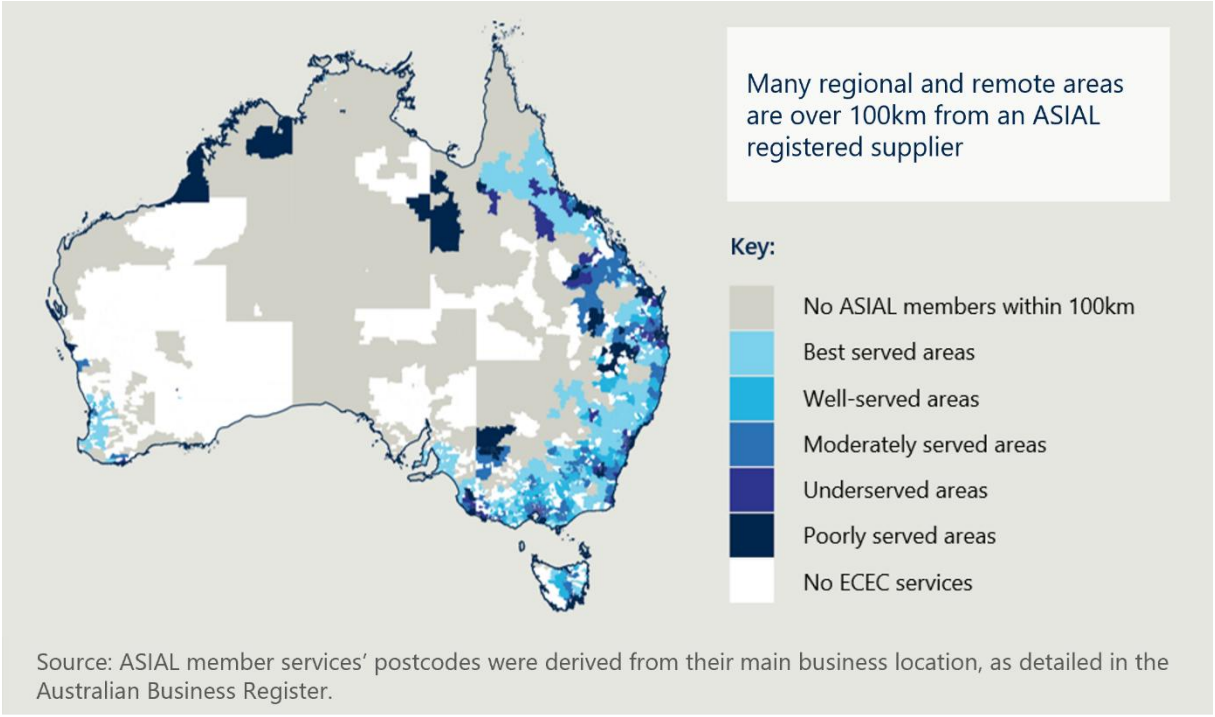
Access: Rural towns (MMM 3-4) rely heavily on distant suppliers. Services in these areas have access to an average of six suppliers within 50km and 39 suppliers within 100km. Several rural and remote postal areas have at least four medium-sized ECEC services,[280] yet are located more than 100km from the nearest ASIAL registered operator.

It is important to note that Figure 13 does not represent all CCTV suppliers nor their precise address, so this analysis should be used as a preliminary illustration of where thin market conditions may exist.[281]

---

[274] IBISWorld, Security System Installation & Monitoring in Australia - Number of Businesses (2021-2031), 2026 (accessed 28 July 2026), https://www.ibisworld.com/australia/number-of-businesses/security-system-installation-and-monitoring/4061/#Faq
[275] ASIAL, About ASIAL, 2026 (accessed 28 July 2026), https://asial.com.au/Web/Web/About-Us/About-Us.aspx
[276] Victoria, ACT and Queensland mandate that security businesses must be members of an approved industry organisation, such as ASIAL.
[277] Derived from a review of ASIAL members identified as providing CCTV sales and installation services, as of July 2026.
[278] Derived from a review of Australian Business Register data of ASIAL members identified as providing CCTV sales and installation services, as of July 2026. The establishment date of a business was defined as its ABN commencement date.
[279] ASIAL, ASIAL Security Industry Licensing Report 2025, 2025 (accessed 28 July 2026), https://securityexpo.com.au/wp-content/uploads/sites/10/2025/06/ASIAL-Security-Licensing-Report-2025.pdf
[280] Medium-sized ECEC services were defined as those with at least 100 approved places.
[281] The ASIAL membership register which captures a large but incomplete share of all CCTV providers (approximately 85 per cent) and precise business operation address are not readily available. Population-weighted postal area centre points are used as a proxy for ECEC service and member locations.

Figure 13 | Relative accessibility of CCTV suppliers to ECEC services nationwide



Source: ASIAL member services' postcodes were derived from their main business location, as detailed in the Australian Business Register.

Services in regional and remote areas face barriers to effective and affordable CCTV installation. It is estimated that limited competition, coupled with increased shipping costs of equipment, place a 10–20 per cent premium on CCTV installation for regional and remote services.[282] Additionally, limited Wi-Fi connectivity in some regional and remote areas may limit the range of available products, as wireless IP cameras require a stable internet connection.

Formal training requirements for CCTV installation licences are limited in most jurisdictions, with more stringent qualifications required for any cabling or electrical work. Licensing requirements vary by jurisdiction and may apply to businesses, individual technicians or both. Licensing requirements may include a combination of: [283]

- **Security licence:** Individuals and businesses that install or maintain CCTV hardware, such as mounting cameras or configuring physical recorders, require a security licence relevant to their jurisdiction, excluding providers operating in Tasmania or the Northern Territory. All security licences require a police background check. Only Western Australia and South Australia require formal training to obtain a licence, and all jurisdictions mutually recognise individual licences. Indicative licensing application processing wait-times range from four weeks (Queensland) to six months (Victoria).284
- **Cabling registration:** Individuals installing or maintaining the data transmission cables for wired IP and analogue camera systems, such as fibre optic or coaxial cables, must be registered with the Australian Communications and Media Authority (ACMA). Individuals performing CCTV cabling generally require an 'Open' licence, which does not restrict the activities cablers can perform. Individuals performing simple cabling tasks may only need a 'Restricted' licence. Open licences take an estimated two and a half months to obtain, relative to an estimated three weeks for Restricted licences, due to a requirement for more supervised experience.

[282] IndexBox, Australia CCTV Camera - Market Analysis, Forecast, Size, Trends and Insights, 1 May 2026 (accessed 28 July 2026), https://www.indexbox.io/store/australia-cctv-camera-market-analysis-forecast-size-trends-and-insights/
[283] See Appendix C for more details on licensing competency requirements across jurisdictions.
[284] Victoria Police, Private security, 27 July 2026 (accessed 28 July 2026), https://www.police.vic.gov.au/private-security; NSW Police Force, Frequently Asked Questions, n.d. (accessed 28 July 2026), https://www.police.nsw.gov.au/online_services/sled/security_licences/frequently_asked_questions; Queensland Government, Apply for a security equipment installer licence, 12 May 2026 (accessed 28 July 2026), https://www.qld.gov.au/community/fair-trading/regulated-industries-licensing-and-legislation/security-industry-regulation/security-technical-licence/apply-for-a-security-equipment-installer-licence

- **Electrical licence:** Individuals performing high-voltage electrical work to power cameras or other CCTV system hardware require an electrical licence relevant to the jurisdiction they are operating in or gain mutual recognition where applicable. Across all jurisdictions, becoming a licensed electrician requires a four-year apprenticeship.

Table 8 details the competency requirements for each licence that may be required to install security camera systems across jurisdictions.

Table 8 | Competency requirements for licences relevant to CCTV installation, by jurisdiction

	NSW	VIC	QLD	WA	SA	TAS	ACT	NT
Individual security installer licence	No formal training required	No formal training required	No formal training required	Complete three vocational education units. **Estimated duration: ~5 days**[285]	Complete applicable Cert II or III qualification. **Estimated duration: ~6 months – 1 year**[286]	*No licence required*	No formal training required	*No licence required*
Business security installation licence	No formal training required	No formal training required	No formal training required	Complete an open-book test. **Estimated duration: ~1 day**[287]	Complete two vocational education units. **Estimated duration: ~6 days**[288]	*No licence required*	No formal training required	*No licence required*
Cabling registration[289]	**Open licence**: Complete 3 vocational education units. Complete a 50-question cabling regulations test. Complete 360 hours of supervised cabling experience. **Estimated total duration: ~2.5 months** **Restricted licence**: Complete 3 vocational education units. Complete a 30-question cabling regulations test. Complete 80 hours of supervised cabling experience. **Estimated total duration: ~3 weeks**							
Electrical licence	Complete relevant work experience and a Cert III qualification. **Estimated total duration: ~4 years.**[290]							

[285] Government of Western Australia, Security licence: training, 20 May 2026 (accessed 28 July 2026), https://www.wa.gov.au/organisation/western-australia-police-force/security-licence-training; Aspire Education and Training, WA Police Licensing (Alarms and CCTV) Training, 2024 (accessed 28 July 2026), https://www.aspire.wa.edu.au/alarms-and-CCTV.php

[286] Consumer and Business Services, Security Agent Qualifications, July 2026 (accessed 28 July 2026), https://cbs.sa.gov.au/documents/security-agent-qualifications.pdf; Department of Employment and Workplace Relations, Certificate II in Technical Security, n.d. (accessed 28 July 2026), https://www.yourcareer.gov.au/learn-and-train/courses/CPP20319

[287] Government of Western Australia, Security licence: application requirements, 16 June 2026 (accessed 28 July 2026), https://www.wa.gov.au/organisation/western-australia-police-force/security-licence-application-requirements

[288] Asset College, SA Security and Investigations Agent (Business Licence), 2026 (accessed 28 July 2026), https://www.asset.edu.au/course/sa-security-and-investigations-agent-business-licence/; Freshstart Education, BSBSMB401, n.d. (accessed 28 July 2026), https://www.freshstart.edu.au/wp-content/uploads/2021/11/BSBSMB401-Course-Brochure.pdf; Inscope Training, QBCC Managerial Course, 2026 (accessed 28 July 2026), https://inscope.edu.au/courses/contractors-business-management-qbcc

[289] Australian Communications and Media Authority, ACMA cabling provider rules, April 2025 (accessed 28 July 2026), https://www.acma.gov.au/sites/default/files/2025-04/ACMA; Milcom, ACMA Open Registration/Cablers Licence, n.d. (accessed 28 July 2026), https://milcom.edu.au/courses/open-registration/

[290] College of Electrical Training, How long is an electrical apprenticeship, 16 April 2025 (accessed 28 July 2026), https://cet.asn.au/news-insights/how-long-is-an-electrical-apprenticeship

Appendix D Regulatory review

CCTV in ECEC is regulated through a combination of Commonwealth, state and territory legislation, privacy frameworks, child safety requirements and provider policy obligations. Figure 14 maps the main legislative instruments covering CCTV use in ECEC services across each jurisdiction.

Figure 14 | Mapping of relevant regulatory instruments across jurisdictions

NSW	VIC	QLD	WA	SA	TAS	ACT	NT
Workplace Surveillance Act 2005						Workplace Privacy Act 2011	
Surveillance Devices Act 2007	Surveillance Devices Act 1999		Surveillance Devices Act 1998	Surveillance Devices Act 2016	Listening Devices Act 1991	Listening Devices Act 1991	Surveillance Devices Act 2007
Privacy and Personal Information Protection Act 1998	Privacy and Data Protection Act 2014	Information Privacy Act 2009	Privacy and Responsible Information Sharing Act 2024		Personal Information Protection 2004	Information Privacy Act 2014	Information Act 2002
Children and Young People (Care and Protection) Act 1998	Children, Youth and Families Act 2005	Child Protection Act 1999	Children and Community Services 2004	Children and Young People (Safety) Act 2017	Children, Young Persons and Their Families Act 1997	Children and Young People Act 2008	Care and Protection of Children Act 2007
Crimes Act 1900	Crimes Act 1958	Crime and Corruption Act 2001	Criminal Code Compilation Act 1913	Criminal Law Consolidation Act 1935	Criminal Code Act 1924	Crimes Act 1900	Criminal Code Act 1983
Education Act 1990	Education and Training Reform Act 2006	Education (General Provisions) Act 2006	School Education Act 1999	Education and Children's Services Act 2019	Education Act 2016	Education Act 2004	Education Act 2015
Criminal Code Act 1995 (Cth)							
Privacy Act 1988 (Cth)							
Education and Care Services National Law and National Regulations							

The National Law is the main legislative instrument regulating ECEC. It does not explicitly include provisions that specifically refer to surveillance devices. Regulation of CCTV derives from the National Regulations and a variety of other state-based laws. However, these latter instruments are not always aligned, which can create challenges for ECEC services who operate across multiple jurisdictions and want to take a consistent approach to CCTV deployment and use. This research has identified eight potential areas of misalignment, grouped into three categories:

- **Gaps** – where legislation and regulations do not provide specific rules related to the use of CCTV in ECEC settings.
- **Inconsistencies** – where legislation and regulations likely preclude ECEC services in one jurisdiction from using CCTV cameras in a similar manner to services in other jurisdictions.
- **Ambiguity** – where legislation and regulations impose a broad obligation but do not specify how that obligation should be applied in ECEC settings.

Key instances of each type of misalignment are described below. Importantly, not all points of difference are problematic; only a subset may benefit from closer consideration.

Gaps

There is no specified mandatory retention period for CCTV footage that does not depict an incident

There is no consistent mandatory retention period for routine CCTV footage. Specific retention or deletion requirements for CCTV footage usually only apply when the footage is relevant to a regulatory investigation or legal proceeding. For example, the Royal Commission into Institutional Responses to Child Sexual Abuse recommended that ECEC services retain records relating to child sexual abuse for at least 45 years.[291]

State and territory legislation sets record keeping requirements for routine footage, but this only applies to government-run ECEC services. Victoria, WA, SA, Tasmania, ACT and NT require footage collected by government organisations to be retained for approximately one month.[292] Queensland and NSW do not specify a retention period, instead requiring footage to be retained until the relevant "administrative or reference use" or "business action" is completed.[293]

General retention requirements for routine CCTV footage, which is considered personally identifiable information, are outlined in the Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth) (Privacy Act).[294] APP 11 requires most ECEC services (the APPs do not apply to most small businesses with turnover less than $3 million per annum) to take reasonable steps to destroy or de-identify personal information once it is not required for its original purpose or under any relevant legislation or court order. However, they do not specify a retention period.

Therefore, most ECEC services must use their discretion to determine how long they should retain routine CCTV footage, as there are no specified mandatory retention periods when an ECEC service is not government-run and the footage must not be retained for a legislative or regulatory purpose. Once footage has reached the end of its retention period, an ECEC service must destroy or de-identify it. The Privacy Act does not prescribe when destruction or de-identification of CCTV footage is more appropriate. OAIC guidance states that de-identification

[291] Royal Commission into Institutional Responses to Child Sexual Abuse, Final Report, Recommendation 8.1
[292] Victorian Government, CCTV in Schools – Installation and Management policy; Western Australian Government, DA 2023-004 General Retention and Disposal Authority for State Government Information, Authority No. 88.3; South Australian Government, State Records of South Australia General Disposal Schedule 40, Item 1.15.6; Tasmanian Government, DECYP CCTV Procedure, p 12; ACT Government, Territory Records (Records Disposal Schedule – Security Coordination Records) Approval 2009 (No 1), Entry No. 182.097.002; NT Government, Safe capture, use, storage and disposal of images and videos of children – procedure.
[293] Queensland Government, General Retention and Disposal Schedule, Disposal Authorisation 1277; NSW Government, Administrative records – Property Management (GA28), Item 16.24.7
[294] Note – the APPs generally do not apply to small businesses (i.e. businesses with an annual turnover less than $3 million). Therefore, some small ECEC services may not be bound by the APPs. State and territory legislation continues to apply to them.

may be more appropriate where the de-identified information could provide further value or utility to the ECEC service or a third-party.[295]

The Privacy Act states that "reasonable steps" to destroy or de-identify information include "technical and organisational measures."[296] OAIC guidance states that examples of technical measures may include shredding, disintegrating and pulping, sanitisation of hardware and de-identification techniques.[297] Examples of organisational measures include staff training, policies and procedures to determine if personal information needs to be retained, destroyed or de-identified, and verifying and documenting when and what personal information is destroyed or de-identified.[298] Separate OAIC guidance outlines two main steps in the de-identification process – first removing direct identifiers, then removing or altering other information that may allow an individual to be identified and/or putting controls and safeguards in place to manage the risk of re-identification.[299] The Privacy Act includes civil penalties for non-compliance with the APPs. A breach carries a penalty of up to 2,000 penalty units ($728,000, as of 1 July 2026), while a "serious" breach carries penalties of up to $2.5 million.[300]

Inconsistencies

Jurisdictions vary in their prescription about camera placement, and none offer a positive standard

There is no positive standard regarding where CCTV cameras can be placed for the purpose of optical surveillance or what they can capture (e.g. field of view). Some jurisdictions define a negative standard (i.e. where CCTV cameras **cannot** be placed), but this standard differs across jurisdictions.

- Victoria, New South Wales and the ACT are the most explicit, **defining specific places where CCTV cameras cannot be placed.** While there is some minor variation between jurisdictions, CCTV cameras are generally prohibited in washrooms, change rooms, bathrooms, toilets, showers and lactation rooms.[301]
- All other jurisdictions (Queensland, Western Australia, South Australia, Queensland, Tasmania and NT) **prohibit the non-party recording of a 'private activity'**, which is broadly defined as an activity where any of the parties to the activity do not wish to be observed and are not in a situation where they would reasonably expect to be observed.[302] The legislation does not identify specific areas that meet this threshold.

Uncertainty regarding what is considered a 'private activity' – namely, in which areas a person would not reasonably expect to be observed – makes it difficult for multi-jurisdictional ECEC providers to rely on a single, national CCTV placement policy. Providers can reasonably assume that some areas are no-camera zones (e.g. bathrooms, change rooms, toilets). However, it is unclear if it is legal in every jurisdiction to install CCTV in other areas (e.g. sleep/nap rooms, staff rooms and first-aid rooms).

Most jurisdictions are less permissive of audio recording than optical recording

In all jurisdictions, the legislative provision related to audio surveillance is different to the one covering visual surveillance. While all jurisdictions allow some optical surveillance with the express or implied consent of the people being filmed, most jurisdictions are less permissive of audio surveillance.

---

[295] Office of the Australian Information Commissioner, Guide to securing personal information, 5 June 2018 (accessed 29 July 2026), https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information

[296] *Privacy Act 1988* (Cth), Schedule 1, s 11https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information

[297] Office of the Australian Information Commissioner, Chapter 11: APP 11 Security of personal information, 3 October 2025 (accessed 27 July 2026), https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information

[298] ibid

[299] Office of the Australian Information Commissioner, De-identification and the Privacy Act, 21 March 2018 (accessed 29 July 2026), https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

[300] *Privacy Act 1988* (Cth), s 13G, s 13H

[301] *Surveillance Devices Act* 1999 (Vic), s 9B; Workplace *Surveillance Act 2005* (NSW), s 15; *Workplace Privacy Act 2011* (ACT), s 41

[302] *Surveillance Devices Act 1998* (WA), s 6; *Criminal Code 1899* (Qld), s 227A; *Surveillance Devices Act 2016* (SA), s 5; *Surveillance Devices Act 2007* (NT), s 12

With some minor variation in wording, all jurisdictions' surveillance legislation defines a private conversation as one where the people in the conversation reasonably expect that their conversation cannot be overhead by anyone else.[303] A non-party recording is where the person operating the surveillance device is not part of the conversation being recorded.[304] Jurisdictions' approach to regulating audio surveillance of private conversations can be grouped as follows:

- NSW, South Australia, Western Australia, Tasmania and the ACT **do not allow non-party recording of private conversations**. Audio recording is allowed for people who are a party to the private conversation with the consent of all other parties to the conversation.[305]
- Queensland takes a similar approach but it **allows audio recording for people who are a party to the private conversation** without needing to receive consent from the other parties.[306]
- Victoria and the Northern Territory are the most permissive. They allow **non-party recording with the express or implied consent of the parties** to the conversation. [307]

A CCTV camera is typically operated by the ECEC service and monitored by managerial staff who are not party to every conversation being captured. Therefore, similar to the uncertainty around the definition of a "private activity" described above, the legality of audio surveillance rests on whether the recording captures a "private conversation". That is, whether "the parties to the conversation ought reasonably to expect that it may be overheard by someone else."[308]

A more expansive interpretation of this definition could allow audio surveillance in most shared spaces (e.g. playrooms, playgrounds). A narrower interpretation could prohibit all audio surveillance except where someone clearly expects to be overheard (e.g. calling out to someone from across a room with others present).

In practice, the Assessment found that a notable minority of services across multiple jurisdictions record audio alongside CCTV footage. Several RAs reported that audio can provide important contextual information that is not captured visually, such as the tone and volume of verbal interactions. However, they also noted that audio recordings share many of the same limitations as visual footage: recordings may be unclear, fail to capture relevant events, or be inconsistent in quality and coverage. Assuming audio surveillance can be recorded with consent, ECEC services must be careful to ensure they receive consent from everyone being recorded, including children, staff and parents.

NSW and ACT have more explicit consent requirements for workplace surveillance

Consent requirements are covered under national, state and territory legislation. Legislation in every jurisdiction requires ECEC services to receive the express or implied consent of the people being recorded to use CCTV cameras. The OAIC states that an organisation must reasonably believe that it has implied consent to collect non-sensitive personal information.[309] APP 3.3 requires organisations to get express consent to collect sensitive information, which OAIC guidance defines as consent which is given openly and obviously, either verbally or in writing.[310]

The National Law does not prescribe specific consent mechanisms for the use of CCTV in ECEC services. The National Regulations require policies and procedures on the safe use of digital technologies and online environments, including the use of optical surveillance devices, the taking, use, storage and destruction of footage of children and the authorisation from parents to take, use and store footage of children.[311] However, they do not

[303] An example of this definition in one jurisdiction's legislation: *Surveillance Devices Act 1999* (Vic), s 3
[304] An example of this definition in one jurisdiction's legislation: *Surveillance Devices Act 2007* (NT), s 4
[305] *Surveillance Devices Act 2016* (SA) s 4; *Surveillance Devices Act 1998* (WA) s 5; *Listening Devices Act 1991* (Tas) s 5; *Listening Devices Act 1992* (ACT) s 4; *Surveillance Devices Act 2007* (NSW) s 7
[306] *Invasion of Privacy Act 1971* (Qld) s 43
[307] *Surveillance Devices Act 1999* (Vic) s 6; *Surveillance Devices Act 2007* (NT) s 11
[308] *Surveillance Devices Act 1999* (Vic) s 3
[309] Office of the Australian Information Commissioner, Consent to the handling of personal information, accessed 29 July 2026, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information
[310] *Privacy Act 1988* (Cth), Schedule 1, s 3
[311] *Education and Care Services National Regulations* (Qld), s 168

prescribe what these policies must include. Therefore, consent requirements are left to jurisdictional legislation, which provide varying degrees of prescription regarding signage and prior notice.

Most jurisdictions (Victoria, Queensland, Western Australia, South Australia, Tasmania and NT) do not specify what actions or measures are required to obtain express or implied consent. The relevant provision in each jurisdiction's surveillance legislation simply requires an ECEC service to receive consent from those being recorded, placing the onus on the service to determine what actions are appropriate to meet this obligation.

There are two jurisdictions (NSW and ACT) with dedicated workplace surveillance laws, which are in addition to general surveillance acts. These prescribe additional consent requirements when surveillance is undertaken in workplaces. In NSW, employee surveillance generally requires at least 14 days' written notice, cameras or camera casings must be clearly visible, and signage must be clearly visible at each entrance to the premises.[312] In the ACT, employers generally must give written notice at least 14 days before surveillance starts. They must consult workers in good faith, ensure optical surveillance devices and signs are clearly visible, and provide workers with access to surveillance records (subject to exceptions such as unlawful disclosure, unreasonable impact on others' privacy or prejudice to an investigation).[313]

The varying prescription of consent and notification requirements across jurisdictions may create uncertainty for ECEC services regarding what they must do to demonstrate that they have received consent to use CCTV cameras. Many large providers have sought external legal advice at significant costs to understand the implications for their CCTV use models.

It is unclear what an ECEC service should do if a parent or staff member does not consent to surveillance that is already in place. The legal implications are likely similar to places like supermarkets and retail stores – that is, the ECEC service retains the right to make CCTV surveillance a condition of entry. The Assessment heard of an instance where a parent did not consent to their child being surveilled. That child was not offered a place at the service.

Ambiguity

ECEC services are uncertain about how they must handle CCTV footage that depicts child abuse

Relevant national, state and territory legislation seeks to protect ECEC services' handling of child abuse material where they are supporting regulatory or police investigations. Legislation is clear that services that record and store unsolicited child abuse material for the purposes of an investigation are not criminally liable. However, the regulations are not clear about how services should share footage with law enforcement, store footage to be used as evidence in a legal proceeding and control access to footage that depicts child abuse. Further detail on these regulatory requirements is provided below:

- **Capture**: All national, state and territory legislation includes provisions that exempt ECEC services from criminal offences related to child abuse material where they did not or could not reasonably have known that the CCTV footage contained child abuse material.[314] It also exempts them from criminal liability if the capture of child abuse material is unsolicited (e.g. where a CCTV camera captures a child unexpectedly undressing).[315]
- **Sharing**: Once child abuse material is identified, ECEC services are also exempt from criminal offences related to the retention and sharing of child abuse materials with the RA as part of an investigation. The time limit on disclosure is clear – child abuse must be disclosed to the relevant RA within 24 hours.[316] However, services reported limited guidance on how they should practically and safely share child abuse material with relevant authorities (i.e. police, child protection or the Regulatory Authority).
- **Use as evidence**: Relevant national, state and territory Evidence Acts do not impose broad obligations on ECEC services to create, store or retain CCTV footage, even where complaints or investigations may hypothetically require them. Relevant Crimes Acts criminalise the destruction of evidence, but this typically falls under

[312] *Workplace Surveillance Act 2005* (NSW), s 10
[313] *Workplace Privacy Act 2011* (ACT), s 13
[314] *Criminal Code Act 1995* (Cth), s 474.24
[315] *Criminal Code Act 1995* (Cth), s 474.22
[316] *Education and Care Services National Regulations* (Qld), s 174, as enabled by the *National Law*, s 301

'perverting the course of justice' and requires intent. There is no criminal liability for failing to follow destruction protocols or for accidental destruction of evidence. Once a clear legal use case has been identified for a piece of footage, then it is considered evidence under the Crimes Acts. There are no legislative requirements related to chain of custody or preservation of metadata.

- **Retention period**: The Royal Commission into Institutional Responses to Child Sexual Abuse recommended that ECEC services retain records relating to child sexual abuse for at least 45 years.[317] While not legally binding, it clearly signals what ECEC services are expected to do to align with best practice.
- **Storage and access**: Services reported uncertainty about how to securely store CCTV footage and appropriately restrict access. For services bound by the APPs, OAIC guidance indicates that 'reasonable steps' to secure personal information will depend on the amount and sensitivity of the information. Therefore, it is reasonable to assume that additional measures, such as additional encryption, logging and auditing of access and strict access controls, would apply to storage of child abuse material.[318]

ECEC services are uncertain about how they can ensure appropriate AI cybersecurity controls

The use of AI in CCTV systems is legally permissible but carries strict consent, notification and security requirements. Many ECEC services face difficulty in determining whether there are sufficient safeguards in place to prevent inappropriate use and disclosure of CCTV footage by AI models. The use of AI can be divided into two key topics – collection and use of information. Each is described in turn.

The collection of biometric information invokes additional consent requirements: ECEC services can capture CCTV footage with cameras that do not have AI capabilities with the implied consent of those being surveilled (e.g. signage saying "CCTV in operation"), as the footage is considered personal information. However, where an AI model uses CCTV cameras to take an electronic copy of biometric information, such as a person's face and voice, for automated verification or identification purposes, this biometric data is considered sensitive information.[319] Sensitive information is generally afforded a higher level of privacy protection than personal information. Collection of sensitive information requires express consent (e.g. an authorisation form). This may create problems for ECEC services that have historically relied on implied consent. In those circumstances, a service would likely need to explicitly request the consent of those that will be surveilled before installing AI functionality. Services would also need to update their policies to clarify how AI is being used.

[317] Royal Commission into Institutional Responses to Child Sexual Abuse, Final Report, Recommendation 8.1
[318] Office of the Australian Information Commissioner, Chapter 11: APP 11 Security of personal information, 3 October 2025 (accessed 27 July 2026), https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information
[319] Office of the Australian Information Commissioner, Facial Recognition Technology: a guide to assessing the privacy risks, 29 July 2026 (accessed 4 August 2026), https://www.oaic.gov.au/__data/assets/pdf_file/0025/266335/Facial-recognition-technology-A-guide-to-assessing-the-privacy-risks-July-2026.pdf

The Bunnings Determination

This case demonstrated that the use of facial recognition technology is legally permissible, but requires stringent consent mechanisms, data security and clear policies to comply with the Privacy Act.

The need to obtain express consent was reinforced by a recent lawsuit. Between 2018 and 2021, Bunnings operated a facial recognition technology (FRT) system in 62 stores in Victoria and NSW. The system, via CCTV, captured the faces of every person who entered the stores and compared them against a database of individuals that Bunnings had identified as posing a risk. Bunnings argued that the use of FRT was sanctioned by "permitted general situations" one and two, which allow for the collection and use of personal information without consent for the purposes of preventing serious safety risks and where there is suspicion of illegal activity related to the organisation's functions or activities.

The Privacy Commissioner found that Bunnings' FRT system had collected sensitive information without consent and Bunnings had not taken reasonable steps to notify people about the way their personal information was being collected and the purpose of collection. Bunnings also failed to maintain clear and up-to-date privacy policies.

This case has important implications for ECEC services looking to use FRT:

- Organisations looking to use FRT must demonstrate that it is necessary. That is, it is effective, there are no available, less intrusive alternative methods and the use of FRT is proportional (the benefits outweigh the privacy risks).
- Organisations must have clear governance arrangements in place, including privacy risk management practices and policies.
- Organisations need to ensure that the biometric information used in FRT Is accurate and steps need to be taken to address any risk of bias.

Source: Office of the Australian Information Commissioner, Bunnings determination, https://www.oaic.gov.au/__data/assets/pdf_file/0027/243936/Bunnings-determination-factsheet.pdf; Case: Appeal: Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130, https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/ARTA/2026/130.html

The use of private information to train AI models requires separate consent: For ECEC services bound by the APPs, APP 6 prohibits personal information that was collected for a particular purpose from being used or disclosed for another purpose without consent.[320] In practice, this means that CCTV footage collected for the purposes of protecting the safety of children and staff cannot then be used to train an AI model unless the ECEC service explicitly receives consent to do so.[321] This includes use of personal information that ECEC services already hold. In practice, this means that ECEC services must explicitly request consent before allowing CCTV footage to train an AI model or ensure that CCTV footage is not unintentionally being used to train a model.

In general, ECEC services must be proactive and deliberate in the way that they seek consent to use AI. That is, they must ensure that they have received express consent for each use case of AI. Services must also have clear access controls for stored footage, so that an AI model does not unintentionally give access to unauthorised third parties. For example, an ECEC service should avoid uploading CCTV footage into a publicly available generative AI tool like ChatGPT. The likely largest regulatory risk of using AI is that insufficient cybersecurity protocols cause a data breach. ECEC services are uncertain about whether and how they can use AI and how to determine whether AI suppliers have appropriately rigorous controls in place.

ECEC services are unsure how to appropriately de-identify footage before sharing it

There is some uncertainty regarding ECEC services' rights and obligations when staff and parents request access to CCTV footage. Generally, access is allowed where ECEC services receive the consent of all those depicted in the footage and de-identify any third parties (i.e. those who did not make the access request). However, it is not clear

[320] *Privacy Act 1988* (Cth), Schedule 1, s 6

[321] Office of the Australian Information Commissioner, Guidance on privacy and developing and training generative AI models, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models

what de-identification measures are appropriate to ensure that ECEC services have not unreasonably impacted on the privacy of others, which can leave ECEC services hesitant to share footage.

Jurisdictional surveillance legislation places restrictions on disclosure. Victoria, NT and Tasmania only allow an ECEC service to communicate or publish a private conversation or private activity with the consent of each party to the conversation or activity.[322] In Queensland, SA, WA and ACT, an ECEC service can also communicate or publish with a party to the conversation or activity without needing the consent of all other parties.[323] NSW does not place restrictions on communication or publication as long as the footage was collected legally.[324]

APP 12 gives individuals a right to access personal information held about them but provides an exception where "giving access would have an unreasonable impact on the privacy of other individuals."[325] This applies to ECEC services that are bound by the APPs. Jurisdictional privacy legislation reinforces this, placing prohibitions on government organisations sharing private information where it impacts the privacy of others. This affects government-run ECEC services but not private services.

ECEC services are uncertain about how to balance a person's right to access their own private information and the service's obligation to protect the privacy of others. Even with the consent of those in the footage, it is unclear if sharing unredacted CCTV footage unfairly impinges on the privacy of third parties (i.e. those who did not make the request for access).

Importantly, there is a means to avoid these privacy impacts. OAIC guidance indicates that information that has undergone an appropriate and robust de-identification process is not personal information and therefore is not subject to the Privacy Act.[326] However, there is uncertainty about how much redaction is sufficient. The Privacy Act does not prescribe a CCTV-specific redaction tool or software standard. OAIC guidance states that determining which specific techniques to use and in what combination depends on the context of the data share or release and may require expert advice.[327]

Case law provides some useful instruction. A 2014 Commonwealth case affirmed that blurring/pixelation is an appropriate de-identification method for CCTV footage, as it adequately obscured the identity of a third-party in the footage so they were not "reasonably identifiable."[328] Two other cases clarified that resource constraints are an important consideration when determining appropriate de-identification. Namely, that de-identification may not be practicable if it places an unreasonable strain on an organisation's resources.[329]

In practice, this means it is likely reasonable for ECEC services to share CCTV footage with parents where all those recorded in the footage have provided consent and are not reasonably identifiable, as long as the de-identification process is not unreasonably burdensome for the ECEC service. For most ECEC services, that do not have the resources or technical knowledge to identify appropriate de-identification measures, the absence of clear guidance can create uncertainty. This is particularly true for sensitive footage, such as incidents or alleged abuse, where there is heightened need to protect the privacy of those in the CCTV footage.

ECEC services can store data on the cloud and overseas but are unsure how to do so safely

There are no explicit bans on the use of cloud-based or offshore storage of CCTV footage, but ECEC services have legal obligations to ensure footage is stored securely. ECEC services need to understand where footage is stored,

[322] *Surveillance Devices Act* (Vic), s 11; *Surveillance Devices Act 2007* (NT) s 15; *Listening Devices Act 1991* (Tas), s 10
[323] *Surveillance Devices Act 2016* (SA) s 27; *Surveillance Devices Act 1998* (WA) s 9; *Listening Devices Act 1992* (ACT) s 5; *Invasion of Privacy Act 1971* (Qld) s 45
[324] *Surveillance Devices Act 2007* (NSW) s 11
[325] *Privacy Act 1988* (Cth), Schedule 1, s 12
[326] Office of the Australian Information Commissioner, De-identification and the Privacy Act, 21 March 2018 (accessed 27 July 2026), https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act
[327] Office of the Australian Information Commissioner, De-identification and the Privacy Act, 21 March 2018 (accessed 27 July 2026), https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act
[328] *'BZ' v Department of Immigration and Border Protection* [2014] AICmr 55
[329] *Willner v Department of Economic Development, Jobs, Training, Resources* [2015] VCAT 669; *Willner v City of Port Phillip* [2015] VCAT 1320;

who can access it, whether it is disclosed outside the relevant jurisdiction, and what contractual, technical and cybersecurity safeguards are in place.

For ECEC services bound by the APPs, APP 11 requires an organisation to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.[330] An organisation is considered to still 'hold' the information if it has possession or control of it, even if it is stored on the cloud or by a third party.[331] OAIC guidance indicates that reasonable measures to ensure cloud storage is secure include implementing effective contractual clauses, verifying security claims of cloud service providers through inspections, and regular reporting and monitoring.[332]

There are additional regulations related to offshore storage and disclosure. For ECEC services bound by the APPs, APP 8 requires organisations to take reasonable steps before disclosing personal information to an overseas recipient to ensure the recipient does not breach the APPs[333], and s16C of the Privacy Act can make the ECEC service legally liable if it discloses personal information to an overseas recipient who subsequently breaches the APPs. OAIC guidance also notes that, even where information is held overseas as a "use" rather than a "disclosure", the organisation remains accountable for relevant APP obligations.[334]

Legislation does not prohibit cloud-based or offshore storage, but it places clear requirements on the secure storage of personal information. The biggest regulatory risk with cloud-based storage of CCTV footage, particularly when stored offshore, is the difficulty in ensuring appropriate cybersecurity measures are in place. This is particularly true for ECEC services that have limited regulatory maturity or technical expertise in data management and storage.

[330] *Privacy Act 1988* (Cth), Schedule 1, APP11
[331] *Privacy Act 1988* (Cth), Schedule 1, s 11
[332] Office of the Australian Information Commissioner, Guide to securing personal information, 5 June 2018 (accessed 28 July 2026),https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information#ftn8
[333] *Privacy Act 1988* (Cth), Schedule 1, s 8
[334] Office of the Australian Information Commissioner, Sending personal information overseas, 13 June 2019 (accessed 3 August 2026), https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/sending-personal-information-overseas

Appendix E Expert Panel

The Assessment was supported by an Expert Panel comprising sector representatives and experts in child protection, privacy, surveillance and law enforcement, including the Australian Centre for Child Protection (ACCP), Office of the Australian Information Commissioner (OAIC) and Australian Federal Police (AFP), which provided advice on the Assessment's design, implementation and interpretation of findings.



Appendix F List of participating providers

Tier 1 and 2 participating services

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Tier 1 participating services				
360 Early Education	360 Early Education Throsby	ACT	2914	Tier 2
360 Early Education	360 Early Education Casey	ACT	2913	Tier 2
360 Early Education	360 Early Education Rivett	ACT	2611	Tier 2
Artemis Early Learning	Artemis Early Learning	ACT	2609	Tier 2
Pinocchio Early Learning Centre	Pinocchio Early Learning Centre Curtin	ACT	2605	Tier 2
Pinocchio Early Learning Centre	Pinocchio Early Learning Centre Dickson	ACT	2602	Tier 2
Aspiring Early Learners	Aspiring Early Learners	NSW	2830	Tier 2
Auburn Kids Learning Academy	Auburn Kids Learning Academy	NSW	2144	Tier 2
Batehaven Early Learning Service	Batehaven Early Learning Service	NSW	2536	Tier 2
Best Start ELC Wadalba	Best Start ELC Wadalba	NSW	2259	Tier 2
Edustellar Pty Ltd	Bright Future Childcare Baulkham Hills	NSW	2153	Tier 2
Edustellar Pty Ltd	Bright Future Childcare Kellyville	NSW	2155	Tier 2
Edustellar Pty Ltd	Bright Future Childcare Doonside	NSW	2767	Tier 2
Empower Early Learning Group Pty Ltd	Empower Early Learning Centre Kingswood	NSW	2747	Tier 2
Empower Early Learning Group Pty Ltd	Empower Early Learning Centre Orchard Hills	NSW	2747	Tier 2
Empower Early Learning Group Pty Ltd	Empower Early Learning Centre Emu Plains	NSW	2750	Tier 2
Essential Early Learning	Essential Early Learning	NSW	2170	Tier 2
Explore & Develop Castlereagh Street, Sydney	Explore & Develop Castlereagh Street, Sydney	NSW	2000	Tier 2
Goodstart Early Learning	Goodstart Elara - Blackstone Street	NSW	2765	Tier 2
Goodstart Early Learning	Goodstart Elara - Harvest Street	NSW	2765	Tier 2
Goodstart Early Learning	Goodstart Glebe	NSW	2037	Tier 2
Goodstart Early Learning	Goodstart Willowdale	NSW	2565	Tier 2
HeartCo Ltd	Hands and Hearts Early Learning Centre Coffs Harbour	NSW	2450	Tier 2
HeartCo Ltd	Hands and Hearts Early Learning Centre Bellingen	NSW	2454	Tier 2
HeartCo Ltd	Hands and Hearts Early Learning Centre Kempsey	NSW	2440	Tier 2

Provider name	Service name	Jurisdiction	Postcode	Participation tier
HopePoint ELC	HopePoint ELC	NSW	2198	Tier 2
Jambra Early Learning	Jambra Early Learning	NSW	2067	Tier 2
Kidopia	Kidopia	NSW	2079	Tier 2
Kids Oasis & Goanna Patch Early Learning	Kids Oasis	NSW	2208	Tier 2
Kids Oasis & Goanna Patch Early Learning	Goanna Patch	NSW	2230	Tier 2
Lilly Pilly South Early Learning Centre	Lilly Pilly South Early Learning Centre	NSW	2452	Tier 2
Little Giggles Early Learning Centre	Little Giggles ELC Woy Woy	NSW	2256	Tier 2
Little Giggles Early Learning Centre	Little Giggles ELC Killarney Vale	NSW	2261	Tier 2
Little Jungle Early Learning Centre	Little Jungle Early Learning Centre	NSW	2117	Tier 2
Little Learners Academy	Little Learners Academy Austral	NSW	2179	Tier 2
Little Learners Academy	Little Learners Academy Rossmore	NSW	2557	Tier 2
Little Learners Academy	Little Learners Academy Lane Cove	NSW	2066	Tier 2
Little Learners Academy	Little Learners Academy Thirlmere	NSW	2572	Tier 2
Nest and Nurture Early Learning	Nest and Nurture Early Learning Centre Baulkham Hills	NSW	2153	Tier 2
Nest and Nurture Early Learning	Nest and Nurture Early Learning Centre Lindfield	NSW	2070	Tier 2
Ocean Shores Preschool	Ocean Shores Preschool	NSW	2483	Tier 2
Padstow Kids Learning Academy	Padstow Kids Learning Academy	NSW	2211	Tier 2
Padstow Kids Learning Academy	Blairmount Kids Learning Academy	NSW	2559	Tier 2
Rainbow Cottage ELC	Rainbow Cottage ELC	NSW	2456	Tier 2
Rise Early Learning	Rise Early Learning Charmhaven	NSW	2263	Tier 2
Rise Early Learning	Rise Early Learning Camperdown	NSW	2050	Tier 2
Sandon Point Children's Centre	Sandon Point Children's Centre	NSW	2516	Tier 2
Seedling Kids	Seedling Kids	NSW	2133	Tier 2
Village Children Winston Hills	Village Children Winston Hills	NSW	2153	Tier 2
Wattle Children Services	Wattle Grove Long Day Care Centre	NSW	2173	Tier 2
Goodstart Early Learning	Goodstart – Darwin Airport	NT	800	Tier 2
Lil' Antz Childcare	Lil' Antz Childcare	NT	870	Tier 2
Bayside Early Learners	Bayside Early Learners	QLD	4655	Tier 2
Bella Grace ELC	Bella Grace Beerwah	QLD	4519	Tier 2
Bella Grace ELC	Bella Grace Brightwater	QLD	4557	Tier 2
Bella Grace ELC	Bella Grace Aroona	QLD	4551	Tier 2

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Bella Grace ELC	Bella Grace Brightwater Kindy	QLD	4551	Tier 2
Bella Grace ELC	Bella Grace Chancellor Park	QLD	4556	Tier 2
Bonnybabes Childcare	Bonny Babes Hope Island	QLD	4212	Tier 2
Bonnybabes Childcare	Bonny Babes Coomera	QLD	4209	Tier 2
Flutterbys Early Development Centre	Flutterbys Early Development Centre	QLD	4035	Tier 2
Goodstart Early Learning	Goodstart Albany Creek - The Boulevard	QLD	4035	Tier 2
Goodstart Early Learning	Goodstart Aspley	QLD	4034	Tier 2
Goodstart Early Learning	Goodstart Bracken Ridge	QLD	4017	Tier 2
Goodstart Early Learning	Goodstart Slacks Creek	QLD	4127	Tier 2
Goodstart Early Learning	Goodstart Griffin	QLD	4503	Tier 2
Goodstart Early Learning	Goodstart Mt Isa	QLD	4825	Tier 2
Gumera Early Learning and Kindergarten	Gumera Early Learning and Kindergarten	QLD	4209	Tier 2
Habitat Early Learning	Habitat Ferny Grove	QLD	4055	Tier 2
Habitat Early Learning	Habitat Nundah	QLD	4012	Tier 2
Habitat Early Learning	Habitat Peregian	QLD	4573	Tier 2
J.A.C's Learning World	J.A.C's Learning World	QLD	4703	Tier 2
Kindred Kids Pty Ltd (trading as Meadow Lane Early Learning)	Meadow Lane Early Learning Maroochydore	QLD	4558	Tier 2
Kindred Kids Pty Ltd (trading as Meadow Lane Early Learning)	Meadow Lane Early Learning Buderim	QLD	4556	Tier 2
Learning Avenues Early Education, Care and Kindergarten	Learning Avenues Early Education, Care and Kindergarten	QLD	4226	Tier 2
Learning Pathways Child Care & Kindergarten	Learning Pathways Child Care & Kindergarten	QLD	4350	Tier 2
Little Locals	Little Locals Auchenflower	QLD	4066	Tier 2
Little Locals	Little Locals Salisbury	QLD	4107	Tier 2
Little Locals	Little Locals Bracken Ridge	QLD	4017	Tier 2
Little Locals	Little Locals Greenbank	QLD	4124	Tier 2
Little Locals	Little Locals South Ripley	QLD	4306	Tier 2
Little Locals	Little Locals Ripley	QLD	4306	Tier 2
Little Locals	Little Locals Collingwood Park	QLD	4301	Tier 2
Little Locals	Little Locals Bundamba	QLD	4304	Tier 2
Little Locals	Little Locals Richlands	QLD	4077	Tier 2
Little Locals	Toowoomba Gardens Early Learning	QLD	4350	Tier 2

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Little Locals	Highfield Gardens Early Learning	QLD	4352	Tier 2
Little Locals	Westbrook Gardens Early Learning	QLD	4350	Tier 2
Rise Early Learning	Rise Early Learning Surfers Paradise	QLD	4217	Tier 2
Sanctuary Early Learning	Sanctuary Early Learning Ashmore	QLD	4214	Tier 2
Sanctuary Early Learning	Sanctuary Early Learning Buderim	QLD	4556	Tier 2
Sanctuary Early Learning	Sanctuary Health and Knowledge Precinct	QLD	4215	Tier 2
Sanctuary Early Learning	Sanctuary Early Learning Adventure Maudsland	QLD	4210	Tier 2
Sanctuary Early Learning	Sanctuary Early Learning Redlynch	QLD	4870	Tier 2
Sparrow Early Learning	Sparrow Early Learning Yarrabilba	QLD	4207	Tier 2
The Hills Montessori Pty Ltd	The Hills Montessori Pty Ltd	QLD	4161	Tier 2
The Learning Garden Child Care & Kindergarten	The Learning Garden Child Care & Kindergarten	QLD	4280	Tier 2
Treehouse Early Learning Centre	Treehouse Early Learning Centre Kingston - Long Day Care	QLD	4114	Tier 2
Treehouse Early Learning Centre	Treehouse Early Learning Centre Lawnton - Long Day Care	QLD	4501	Tier 2
Treehouse Early Learning Centre	Treehouse Early Learning Centre Pimpama - Long Day Care	QLD	4209	Tier 2
Treehouse Early Learning Centre	Treehouse Early Learning Centre Camira - Long Day Care	QLD	4300	Tier 2
Treehouse Early Learning Centre	Tree of Life Childcare Centre and Kindergarten	QLD	4213	Tier 2
Department for Education South Australia - Preschools and Early Childhood Services	Morphett Vale Preschool	SA	5162	Tier 2
Department for Education South Australia - Preschools and Early Childhood Services	Para Hills Preschool	SA	5096	Tier 2
Goodstart Early Learning	Goodstart Cowandilla	SA	5033	Tier 2
Goodstart Early Learning	Goodstart Rostrevor	SA	5072	Tier 2
Lower Eyre Peninsula Community Childcare Services Inc	Toybox Community Child Care Centre	SA	5606	Tier 2
Unity College Early Learning Centre	Unity College Early Learning Centre	SA	5253	Tier 2
Woodville Day Nursery	Woodville Day Nursery	SA	5011	Tier 2
Arthur St Early Learning as Trustee for Sorell Child Care Trust	Arthur St Early Learning	TAS	7172	Tier 2
A2Z Childcare and Kindergarten	A2Z Childcare and Kindergarten	VIC	3081	Tier 2

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Abeles Liberman Pre School	Abeles Liberman Pre-School (Caulfield South)	VIC	3162	Tier 2
Bright Start Childcare and Early Learning Centre	Bright Start Childcare and Early Learning Centre	VIC	3280	Tier 2
Flutterbys Early Development Centre	Child's Play Tarneit	VIC	3029	Tier 2
Child's Play ELC	Child's Play Tarneit West	VIC	3029	Tier 2
Child's Play ELC	Child's Play Torquay	VIC	3228	Tier 2
Child's Play ELC	Child's Play Point Cook	VIC	3030	Tier 2
Child's Play ELC	Child's Play Mambourin	VIC	3024	Tier 2
Child's Play ELC	Child's Play Wyndham Vale	VIC	3024	Tier 2
Child's Play ELC	Child's Play Truganina	VIC	3029	Tier 2
Child's Play ELC	Child's Play Dandenong	VIC	3175	Tier 2
Goodstart Early Learning	Goodstart Caulfield	VIC	3162	Tier 2
Goodstart Early Learning	Goodstart Delacombe (Ballarat)	VIC	3356	Tier 2
Goodstart Early Learning	Goodstart Mount Clear	VIC	3350	Tier 2
Goodstart Early Learning	Goodstart Richmond	VIC	3121	Tier 2
Goodstart Early Learning	Goodstart Rosanna - Bellevue Ave	VIC	3084	Tier 2
Goodstart Early Learning	Goodstart Ballarat - Creswick Road	VIC	3350	Tier 2
Goodstart Early Learning	Goodstart Wendouree	VIC	3355	Tier 2
Goodstart Early Learning	Goodstart Thornbury – Hutton Street	VIC	3071	Tier 2
Goodstart Early Learning	Goodstart Forest Hill	VIC	3131	Tier 2
Happy Sprouts Early Learning Beveridge	Happy Sprouts Early Learning Beveridge	VIC	3753	Tier 2
Josie's Bright Beginnings	Josie's Bright Beginnings	VIC	3037	Tier 2
KIKA Investments Pty Ltd	Kids World Werribee	VIC	3030	Tier 2
Leading Bees Montessori	Leading Bees Montessori & Early Learning Templestowe	VIC	3106	Tier 2
Leading Bees Montessori	Leading Bees Montessori & Early Learning Boronia	VIC	3155	Tier 2
Little Penguin Kilsyth Pty Ltd	Little Penguin Kilsyth Pty Ltd	VIC	3137	Tier 2
Me for Kids Croydon Pty Ltd	Me for Kids Croydon	VIC	3136	Tier 2
Me for Kids Lalor Pty Ltd	Me for Kids Lalor	VIC	3075	Tier 2
Me for Kids Pty Ltd	Me for Kids Thomastown	VIC	3074	Tier 2
My Stars Essendon	My Stars Berwick Early Learning Centre	VIC	3806	Tier 2
My Stars Essendon	My Stars Essendon Early Learning Centre	VIC	3040	Tier 2

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Nicki's Clever Cookies	Nicki's Clever Cookies	VIC	3070	Tier 2
Playmakers Early Learning	Playmakers Early Learning	VIC	3028	Tier 2
Precious Seeds Early Learning Pty Ltd	Precious Seeds Early Learning Hallam	VIC	3803	Tier 2
Ready Set Go	Ready Set Go Mortlake	VIC	3272	Tier 2
Wise Kids ELC	Wise Kids ELC	VIC	3820	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Swan View	WA	6056	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare East Byford	WA	6122	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Bertram	WA	6167	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Two Rocks	WA	6037	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Byford	WA	6122	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Kelmscott	WA	6111	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Thornlie	WA	6108	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Carlisle	WA	6101	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Beckenham	WA	6107	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Canning Vale	WA	6155	Tier 2
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Southlake	WA	6164	Tier 2
Goodstart Early Learning	Goodstart Perth Kaadidjiny Maya	WA	6000	Tier 2
Goodstart Early Learning	Goodstart Sinagra	WA	6065	Tier 2
Goodstart Early Learning	Goodstart Albany	WA	6330	Tier 2
Tier 1 participating services				
Bright Bees Early Learning (Nicholls) Pty Ltd	Blooming Buds Early Learning Centre	ACT	2912	Tier 1
Bright Bees Early Learning (Nicholls) Pty Ltd	Buds and Bees Early Learning Centre	ACT	2617	Tier 1
Bright Bees Early Learning (Nicholls) Pty Ltd	Cubs Corner Early Learning Pty Ltd	ACT	2900	Tier 1
Bright Bees Early Learning (Nicholls) Pty Ltd	Bright Buds Early Learning	ACT	2609	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Bright Future Early Learning Belconnen	Bright Future Early Learning Belconnen	ACT	2617	Tier 1
Community Services 1	Forrest Early Education & Care	ACT	2603	Tier 1
Community Services 1	Marlee Early Education & Care	ACT	2604	Tier 1
St Nicks Early Learning	St Nicks Hellenica	ACT	2600	Tier 1
St Nicks Early Learning	St Nicks Botanica	ACT	2600	Tier 1
Wonderschool	Wonderschool Conder	ACT	2906	Tier 1
Wonderschool	Wonderschool Dickson	ACT	2602	Tier 1
Wonderschool	Wonderschool Monash	ACT	2904	Tier 1
Wonderschool	Wonderschool Taylor	ACT	2913	Tier 1
Wonderschool	Wonderschool Throsby	ACT	2914	Tier 1
Wonderschool	Wonderschool Woden	ACT	2606	Tier 1
Inverell District Family Services	Baby Sprouts	NSW	2360	Tier 1
Inverell District Family Services	Catherine Campbell Long Day Care	NSW	2360	Tier 1
Inverell District Family Services	IDFS Ashford Preschool	NSW	2361	Tier 1
Inverell District Family Services	Jack & Jill Preschool Inverell	NSW	2360	Tier 1
Inverell District Family Services	Little Sprouts Learning Centre	NSW	2360	Tier 1
Inverell District Family Services	Tingha Preschool	NSW	2369	Tier 1
Inverell District Family Services	Kindamindi Preschool	NSW	2360	Tier 1
Adventures Preschool & LDC	Adventures Preschool & LDC West Pennant Hills	NSW	2125	Tier 1
Adventures Preschool & LDC	Adventures Preschool & LDC Pennant Hills	NSW	2120	Tier 1
Adventures Preschool & LDC	Adventures Preschool & LDC Turramurra	NSW	2074	Tier 1
Amigoss Spanish Bilingual Childcare	Amigoss Spanish Bilingual Childcare	NSW	2037	Tier 1
Belrose Kindergarten	Belrose Kindergarten	NSW	2085	Tier 1
Bright Bees Early Learning (Nicholls) Pty Ltd	Bright Blooms ELC PTY LTD	NSW	2065	Tier 1
Bumblebee Academy Punchbowl	Bumblebee Academy Punchbowl	NSW	2197	Tier 1
Clovelly Childcare Centre	Clovelly Childcare Centre	NSW	2031	Tier 1
Davbark Pty Ltd	Blair Athol Child Care Centre and Pre-School	NSW	2560	Tier 1
Davbark Pty Ltd	Englorie Park Child Care Centre & Pre-School	NSW	2560	Tier 1
Dooral Kenthurst Early Learning Centre	Dooral Kenthurst Early Learning Centre	NSW	2156	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Enchanted Castle Child Care Centre	Enchanted Castle Child Care Centre	NSW	2190	Tier 1
Fair Play OOSH	Fair Play OOSH Edgeworth	NSW	2285	Tier 1
Footprints Erina Limited	Footprints Erina Limited	NSW	2250	Tier 1
Golden Valley Childrens Learning Centre	Golden Valley Childrens Learning Centre	NSW	2756	Tier 1
Jerilderie Early Learning Centre	Jerilderie Early Learning Centre	NSW	2716	Tier 1
Kids Planet Academy	Kids Planet Academy	NSW	2113	Tier 1
Kids Planet Academy	Kids Planet Academy West Pennant Hills	NSW	2125	Tier 1
Kidz Care Kindergarten Pty Ltd	Kidz Care Kindergarten Pty Ltd	NSW	2761	Tier 1
Koorana Child and Family Services	Koorana Child and Family Services Roselands - Phillip Street Preschool	NSW	2196	Tier 1
Koorana Child and Family Services	Koorana Child and Family Services Lakemba - Croydon Street Preschool	NSW	2195	Tier 1
Little Scholars Academy	Little Scholars Academy - Fairy Meadow	NSW	2519	Tier 1
Little Scholars Academy	Little Scholars Academy - Lake Heights	NSW	2502	Tier 1
Lochinvar Learning Early Education, Care and Preschool	Lochinvar Learning Early Education, Care and Preschool	NSW	2321	Tier 1
Merrylands Christian Preschools Assoc	St Anne's Preschool	NSW	2160	Tier 1
Merrylands Christian Preschools Assoc	St Thomas' Preschool	NSW	2160	Tier 1
Mini Wonders Pty Ltd	Mini Wonders Pty Ltd	NSW	2117	Tier 1
Monash Preschool and Early Learning	Monash Preschool and Early Learning	NSW	2145	Tier 1
My First School Childcare Centre	My First School Childcare Centre	NSW	2760	Tier 1
Peter Pan Preschool	Peter Pan Preschool	NSW	2340	Tier 1
Picnic Point Preschool and Childcare Centre	Picnic Point Preschool and Childcare Centre	NSW	2213	Tier 1
Stepping Stones Early Learning Centres	Stepping Stones ELC Bexley	NSW	2207	Tier 1
Stepping Stones Early Learning Centres	Stepping Stones ELC Kirrawee	NSW	2232	Tier 1
The Discovery Garden Child Care Centre and Preschool	The Discovery Garden Child Care Centre and Preschool	NSW	2280	Tier 1
The Learning Terrace Child Care Centre and Preschool	The Learning Terrace Child Care Centre and Preschool	NSW	2324	Tier 1
The Little Learning Tree	The Little Learning Tree	NSW	2790	Tier 1
Three Little Birds Early Learning Centre	Three Little Birds Early Learning Centre	NSW	2067	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Tongarra Road Preschool and Early Learning Centre	Tongarra Road Preschool and Early Learning Centre	NSW	2527	Tier 1
ValdaEna Pty Ltd (Bright Start Preschool)	ValdaEna Pty Ltd (Bright Start Preschool)	NSW	2261	Tier 1
Wombat Occasional Child Care Inc.	Wombat Occasional Child Care Inc.	NSW	2228	Tier 1
Woodgreen Early Learning Centre	Woodgreen Early Learning Centre	NSW	2135	Tier 1
Creative Early Learning Group Pty Ltd	Creative Kids at Bundaberg	QLD	4670	Tier 1
Creative Early Learning Group Pty Ltd	Creative Kids at Bargara	QLD	4670	Tier 1
Ace Academy Early Learning	Ace Academy Early Learning Morayfield	QLD	4507	Tier 1
Ace Academy Early Learning	Ace Academy Early Learning Morayfield East	QLD	4506	Tier 1
Bamagau Kazil Torres Strait Islanders Corporation	Ama Lala Daycare	QLD	4876	Tier 1
Centenary Childcare & Early Education Centre	Centenary Childcare & Early Education Centre	QLD	4074	Tier 1
GDMP Childcare Pty Ltd	GDMP Childcare Pty Ltd	QLD	4568	Tier 1
Gumnuts on Hardys Rd	Gumnuts on Hardys Rd	QLD	4213	Tier 1
Ipswich Girls' Grammar including Ipswich Junior Grammar Early Education Centre	Ipswich Girls' Grammar including Ipswich Junior Grammar Early Education Centre	QLD	4305	Tier 1
Kidventure Early Learning Eagleby	Kidventure Early Learning Eagleby	QLD	4207	Tier 1
Lady Gowrie Qld Ltd	Lady Gowrie Thursday Island Child Centre	QLD	4875	Tier 1
Lady Gowrie Qld Ltd	Lady Gowrie Dysart Child Centre	QLD	4745	Tier 1
Little Wishes Early Learning Centres Carina and Chermside	Little Wishes Early Learning Centre Chermside	QLD	4032	Tier 1
Little Wishes Early Learning Centres Carina and Chermside	Little Wishes Early Learning Centre Carina	QLD	4152	Tier 1
Littlies Group Pty Ltd	Littlies Group Pty Ltd	QLD	4350	Tier 1
Nest Montessori Children's House	Nest Montessori Children's House	QLD	4053	Tier 1
Noble Nest Early Learning Centre	Noble Nest Early Learning Centre	QLD	4208	Tier 1
Oceans Group Pty Ltd	Elm Tree Early Learning	QLD	4208	Tier 1
Oceans Group Pty Ltd	Starkids Early Learning	QLD	4305	Tier 1
Oceans Group Pty Ltd	1234 Kids	QLD	4306	Tier 1
Oceans Group Pty Ltd	D'Aguilar Early Learning	QLD	4514	Tier 1
Okinja Early Learning Centre & Kindergarten	Okinja Early Learning Centre & Kindergarten	QLD	4570	Tier 1
Port Kennedy Association Inc	Port Kennedy Association Inc	QLD	4875	Tier 1
Sparrow Early Learning	Sparrow Early Learning Ferny Grove	QLD	4055	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
St Mark's Lutheran Early Learning Centre	St Mark's Lutheran Early Learning Centre	QLD	4122	Tier 1
The NEST Early Education Centre	The NEST Early Education Centre	QLD	4215	Tier 1
The Willows Outside School Hours Care	The Willows Outside School Hours Care	QLD	4817	Tier 1
Beyond Early Learning	Beyond Early Learning Goolwa	SA	5214	Tier 1
Beyond Early Learning	Beyond Early Learning Blackwood	SA	5050	Tier 1
Beyond Early Learning	Beyond Early Learning Mount Gambier	SA	5291	Tier 1
Port Augusta City Council	Port Augusta City Council Childcare Centre	SA	5700	Tier 1
Sunrise Christian School Early Learning Centres	Sunrise Christian School Whyalla Early Learning Centre	SA	5608	Tier 1
Sunrise Christian School Early Learning Centres	Sunrise Paradise Early Learning Centre	SA	5075	Tier 1
Sunrise Christian School Early Learning Centres	Sunrise Marion Early Learning Centre	SA	5043	Tier 1
Sunrise Christian School Early Learning Centres	Sunrise Fullarton Early Learning Centre	SA	5063	Tier 1
Sunrise Christian School Early Learning Centres	Sunrise Morphett Vale Early Learning Centre	SA	5162	Tier 1
Adventure Patch	Mountain View Kingston	TAS	7050	Tier 1
Adventure Patch	Ocean View Blackmans Bay	TAS	7052	Tier 1
Adventure Patch	Roland View Sheffield	TAS	7306	Tier 1
Adventure Patch	Blackmans Bay OSHC	TAS	7052	Tier 1
Adventure Patch	Kingston OSHC	TAS	7050	Tier 1
Alphington Early Learning Centre	Alphington Early Learning Centre	VIC	3078	Tier 1
Bursaria Early Learning Centre	Bursaria Early Learning Centre	VIC	3036	Tier 1
G1 Early Education Pty Ltd	Creative Hands Early Learning Centre	VIC	3030	Tier 1
Hoppers Crossing Montessori Centre	Hoppers Crossing Montessori Centre	VIC	3029	Tier 1
Hoppers Crossing Montessori Centre	Montessori Minds Childcare Centre	VIC	3214	Tier 1
Mandalay Early Learning Centre	Mandalay Early Learning Centre	VIC	3753	Tier 1
Montessori Steps Noble Park	Montessori Steps Noble Park	VIC	3174	Tier 1
Moresby Ave Childcare & ELC	Moresby Ave Childcare & ELC	VIC	3105	Tier 1
Red Apple Early Learning Centre	Red Apple Early Learning Centre Balwyn	VIC	3104	Tier 1
Redspire Pty Ltd	Redspire Pty Ltd	VIC	3089	Tier 1
Rivergum Early Learning Centre	River Gum Early Learning	VIC	3082	Tier 1
Rivergum Early Learning Centre	Kiddy Palace Learning	VIC	3076	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Rosebud West Community Hub Ltd (T/A Seawinds Early Learning Centre)	Rosebud West Community Hub Ltd (T/A Seawinds Early Learning Centre)	VIC	3939	Tier 1
Sparrow Early Learning	Sparrow Early Learning Stratford	VIC	3862	Tier 1
WP Early Learning Pty Ltd	WattlePlanet Early Learning Centre	VIC	3152	Tier 1
WP Early Learning Pty Ltd	WattlePlanet Early Learning Centre Vermont South	VIC	3133	Tier 1
WP Early Learning Pty Ltd	WattlePlanet Early Learning Centre Learning Rockbank	VIC	3335	Tier 1
Craigie Early Learning Centre	Craigie Early Learning Centre	WA	6025	Tier 1
Cuddles Early Learning & Childcare	Cuddles Early Learning & Childcare Beechboro	WA	6063	Tier 1
Daisy Child Care Pty Ltd	Bush Kids WA	WA	6232	Tier 1
Daisy Child Care Pty Ltd	Bush Kids Busselton	WA	6280	Tier 1
Daisy Child Care Pty Ltd	Bush Kids Bunbury	WA	6230	Tier 1
Daisy Child Care Pty Ltd	Bush Kids on Sanford	WA	6232	Tier 1
Growzone - Guildford Early Learning Centre	Growzone - Guildford Early Learning Centre	WA	6056	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Beechboro	WA	6063	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Coolbellup	WA	6163	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Ballajura	WA	6066	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga High Wycombe	WA	6057	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Hilton	WA	6163	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Woodvale	WA	6026	Tier 1
Meerilinga Children and Community Services Incorporated	Meerilinga Kingsley	WA	6026	Tier 1
Montessori Stepping Stones	Montessori Stepping Stones	WA	6164	Tier 1
Shire of Mundaring	Midvale Early Childhood and Parenting Centre	WA	6056	Tier 1
Stride Group Pty Ltd	Stride Early Learning Ashby	WA	6065	Tier 1
Stride Group Pty Ltd	Stride Early Learning Baldivis	WA	6171	Tier 1
Stride Group Pty Ltd	Stride Early Learning Bayswater	WA	6053	Tier 1
Stride Group Pty Ltd	Stride Early Learning Belmont	WA	6105	Tier 1
Stride Group Pty Ltd	Stride Early Learning Coolbellup	WA	6163	Tier 1

Provider name	Service name	Jurisdiction	Postcode	Participation tier
Stride Group Pty Ltd	Stride Early Learning Dayton	WA	6055	Tier 1
Stride Group Pty Ltd	Stride Early Learning Karrinyup	WA	6018	Tier 1
Stride Group Pty Ltd	Stride Early Learning Midland	WA	6056	Tier 1
Stride Group Pty Ltd	Stride Early Learning Perth CBD	WA	6000	Tier 1
Stride Group Pty Ltd	Stride Early Learning Wattle Grove	WA	6107	Tier 1
Stride Group Pty Ltd	Stride Early Learning Ardross	WA	6153	Tier 1
Stride Group Pty Ltd	Stride Early Learning Brabham	WA	6055	Tier 1

Large provider participation

Outside of services that actively participated in Tier 2 of the Assessment, several large providers also contributed insights at various stages of the Assessment process. These providers included:

- Affinity Education
- Goodstart Early Learning *(also provided 25 of their services as participants in Tier 2 – see above)*
- Guardian Childcare and Education
- G8 Education
- Montessori Academy
- Sparrow Early Learning

Appendix G Composition of Assessment participation

Table 9 | Jurisdiction of participating services

Jurisdiction	Tier 1 services	Tier 2 services
ACT	21	6
NSW	92	44
NT	2	2
QLD	77	50
SA	16	7
TAS	6	1
VIC	53	36
WA	42	14

The Assessment cohort was broadly representative by jurisdiction, although some jurisdictions were over- or underrepresented relative to their share of services nationally:

- Australian Capital Territory was overrepresented by 4.8 per cent
- New South Wales was underrepresented by 4.2 per cent
- Northern Territory was underrepresented by 0.7 per cent
- Queensland was overrepresented by 7 per cent
- South Australia was underrepresented by 2.6 per cent
- Tasmania was overrepresented by 0.5 per cent
- Victoria was underrepresented by 10.4 per cent
- Western Australia was overrepresented by 5.5 per cent

Table 10 | Remoteness of participating services

Remoteness[335]	Tier 1 services	Tier 2 services
Metropolitan	235	124
Regional	35	18
Rural	33	15
Remote	6	3

The Assessment cohort was slightly skewed towards metropolitan services, while regional and remote services closely reflected the national distribution:

- Metropolitan services were overrepresented by 7 per cent

[335] The Assessment classified service remoteness using the Modified Monash Model (https://www.health.gov.au/topics/rural-health-workforce/classifications/). In contrast, the analysis of the representativeness of Tier 1 services used a separate, but broadly comparable, Australian Bureau of Statistics geographic classification framework (https://www.abs.gov.au/statistics/standards/australian-statistical-geography-standard-asgs/latest-release)

- Regional services were overrepresented by 0.3 per cent
- Rural services were underrepresented by 6.3 per cent
- Remote services were underrepresented by 0.5 per cent

Table 11 | Service type of participating services

Service type	Tier 1 services	Tier 2 services
Long Day Care	292	155
Outside School Hours Care	3	0
Preschool / Kindergarten	14	5

The Assessment cohort overrepresented Long Day Care services and underrepresented other service types:

- Long Day Care services were overrepresented by 42.9 per cent
- Outside School Hours Care services were underrepresented by 25.2 per cent
- Preschool/Kindergarten services were underrepresented by 12 per cent

Table 12 | Ownership type among participating services

Ownership type	Tier 1 services	Tier 2 services
Community-based	13	3
Government / Not for profit	64	32
Private	232	125

The Assessment cohort was skewed towards privately operated services, with community-based and government/not-for-profit providers underrepresented:

- Community-based services were underrepresented by 9.2 per cent
- Private services were overrepresented by 20 per cent
- Government/not-for-profit services were underrepresented by 7.9 per cent

Table 13 | Provider size among participating services

Provider size	Tier 1 services	Tier 2 services
Small (single service)	74	30
Medium (two to 24 services)	203	102
Large (25+ services)	32	28

The Assessment cohort underrepresented large providers and overrepresented small and medium-sized providers:

- Large providers were underrepresented by 30.5 per cent
- Medium providers were overrepresented by 16.0 per cent
- Small providers were overrepresented by 14.5 per cent