



Australian Government  
Department of Education

# PRISMS API Services Terms of Use for Education Providers

Provider Registration and International Student  
Management System (PRISMS)



# Contents

PRISMS API Services Terms of Use for Education Providers.....	1
PRISMS API Services Terms of Use – Education Providers .....	3
1. About these Terms.....	3
2. Provider Access to the PRISMS API Services.....	5
3. Use of the PRISMS API Services .....	7
4. Provider reporting obligations.....	7
5. Privacy.....	8
6. Security and data protection .....	9
7. Technical Support .....	9
8. Continuity of access .....	9
9. Circumstances to be notified to the Department.....	10
10. Intellectual property .....	10
11. Liability and indemnity.....	11
12. Suspension and termination of access.....	11
13. Auditing .....	12
14. Governing law .....	13
15. Execution.....	13

# PRISMS API Services Terms of Use – Education Providers

---

## 1. About these Terms

1.1 In these Terms, a reference to:

- (a) **Applicable PRISMS-Integrated Software** has the meaning given in clause 0.
- (b) **Change in Control** means:
  - (i) a body corporate or entity that Controls the Provider ceases to Control the Provider; or
  - (ii) a body corporate or entity that does not Control the Provider comes to Control the Provider.
- (c) **Client ID(s)** means the unique identifier created by the Department which allows a Provider to use the PRISMS API with a specific Recognised PRISMS Integrated Software. Each Recognised PRISMS Integrated Software used by a Provider requires its own Client ID.
- (d) **Control** means, in relation to the Provider in the context of a Change in Control, any of the following:
  - (i) the ability to exercise or control the exercise of the right to vote in respect of more than 50% of the voting shares or other form of voting equity in the Provider;
  - (ii) the ability to dispose or exercise control over the disposal of more than 50% of the shares or other form of equity in the Provider;
  - (iii) the ability to appoint or remove a majority of the directors of the Provider;
  - (iv) the ability to exercise or control the exercise of the casting of a majority of votes at the meeting of the board of directors of the Provider; and
  - (v) any other means, direct or indirect, of dominating the decision making and financial and operating policies of the Provider.
- (e) **Cyber Security Assessment** is a reference to the evaluation used by the Department to ensure the Provider meets the security standards set out in the Right Fit for Risk Cyber Security Accreditation Framework.
- (f) **Cyber Security Assessment Outcome** means the rating given to the Provider as a result of a Cyber Security Assessment, reflecting the level of cyber security risk associated with the Provider.

- (g) **CRICOS** means Commonwealth Register of Institutions and Courses for Overseas Students.
- (h) **Department** is a reference to the Commonwealth of Australia as represented by the Department of Education.
- (i) **Eligible Data Breach** has the same meaning as in the Privacy Act.
- (j) **ESOS Act** is a reference to the *Education Services for Overseas Students Act 2000* (Cth).
- (k) **Personal Information** has the same meaning as in the Privacy Act.
- (l) **PRISMS** means the Department's Provider Registration and International Student Management System.
- (m) **PRISMS API** is a reference to the Department's application programming interface for PRISMS that allows education providers to access and enter information into PRISMS for the purposes of section 109 of the ESOS Act.
- (n) **PRISMS API Portal** is a reference to the online platform provided by the Department and accessible at <https://portal.api.prisms.education.gov.au/> (or such other website as notified by the Department from time to time) to enable software vendors and education providers to access, discover, and learn about the PRISMS API Services.
- (o) **PRISMS API Services** is a reference to:
  - (i) the PRISMS API;
  - (ii) the PRISMS Production Environment; and
  - (iii) the PRISMS API Portal.
- (p) **PRISMS API Services Hub** is a reference to the Department's website accessible at <https://www.education.gov.au/prisms-api-services-hub> (or such other website as notified by the Department from time to time), which provides general information about the PRISMS API Services, including:
  - (i) updates, news and communications; and
  - (ii) the process for software vendors and education providers to gain access to the PRISMS API Services.
- (q) **PRISMS Production Environment** is a reference to the live environment in which education providers access and enter information for the purposes of section 109 of the ESOS Act via Recognised PRISMS-Integrated Software.
- (r) **Privacy Act** means the *Privacy Act 1988* (Cth).
- (s) **Provider** is a reference to the entity agreeing to these Terms whose details are set out in the Provider Details section of these Terms.

- (t) **Provider Personnel** is a reference to Provider officers, employees, contractors, agents and any other person over whom the Provider exercise control or direction.
  - (u) **Recognised PRISMS-Integrated Software** means a software application that has been recognised by the Department as having successfully completed integration with PRISMS in the PRISMS staging environment and which meets the required standards to connect to the PRISMS Production Environment.
  - (v) **Right Fit for Risk Cyber Security Accreditation Framework** means the framework developed by the Commonwealth Department of Employment and Workplace Relations (DEWR) as amended from time to time which the Department uses for the Cyber Security Assessment.
  - (w) **Terms** means these PRISMS API Terms of Use as amended from time to time in accordance with clause 0.
  - (x) **Vendor** is a reference to an entity that develops, licences or supplies Applicable Recognised PRISMS-Integrated Software to the Provider.
- 1.2 These Terms set out the basis on which the Provider undertakes to access the PRISMS API Services. The Provider acknowledges and agrees that if the Department provides it with access to the PRISMS API Services in accordance with these Terms, that access is given to the Provider in consideration of its agreement to these Terms.
- 1.3 The Department may amend these Terms with at least 3 days' notice to the Provider which:
- (a) sets out the updated Terms; and
  - (b) the date that updated Terms will take effect.
- 1.4 The parties acknowledge and agree that the Department may provide a notice under clause 0 by:
- (a) publishing the updated Terms on the PRISMS API Portal or PRISMS API Services Hub; or
  - (b) sending the updated Terms to the Provider's e-mail address (as set out in the Provider Details section of these Terms or as otherwise updated by the Provider).
- 1.5 If the Provider accesses or uses the PRISMS API Services after the notice period, it will be taken to agree to the amended Terms.
- 

## 2. Provider Access to the PRISMS API Services

- 2.1 As at the commencement of these Terms, the Provider has submitted a request to the Department seeking access to:
- (a) the PRISMS API Portal; and

- (b) the PRISMS API via one or more of the Provider's nominated Recognised PRISMS-Integrated Software (**Applicable Recognised PRISMS-Integrated Software**),

and the Provider represents and warrants to the Department that any information the Provider has provided, or will provide, to the Department is true, complete and accurate.

- 2.2 The Department will review the Provider's request and any other relevant information to determine whether the Provider:
    - (a) satisfies the eligibility criteria for access to the PRISMS API Services by education providers (available on the PRISMS API Services Hub or as otherwise notified by the Department and as amended from time to time); and
    - (b) has a Cyber Security Risk Outcome of a suitable standard as determined by the Department.
  - 2.3 The Department will determine (at its sole discretion) whether to grant or refuse the Provider or Provider Personnel access to:
    - (a) the PRISMS API via the Applicable Recognised PRISMS-Integrated Software; and
    - (b) the PRISMS API Portal.
  - 2.4 The Department may grant the Provider (and Provider Personnel) access under clause 0 subject to conditions that are in addition to the conditions set out in these Terms, and the Provider must comply with those conditions. The Department will notify the Provider of the outcome of its application but is not required to provide reasons for its decision.
  - 2.5 Access granted to the Provider under clause 0 is limited to the Applicable Recognised PRISMS-Integrated Software that was the subject of the Provider's request. If the Provider seeks to access the PRISMS API via different Recognised PRISMS-Integrated Software, the Provider must submit a new request to the Department, in the form prescribed on the PRISMS API Services Hub, in which case the process in clauses 0 to 0 above (as it relates to access to the PRISMS API) applies in respect of that different nominated Recognised PRISMS-Integrated Software.
  - 2.6 In granting a Provider access to the PRISMS API via a new Applicable Recognised PRISMS-Integrated Software under clause 0, the Department may vary the Provider's access to the PRISMS API by withdrawing the Provider's access via any existing Applicable Recognised PRISMS-Integrated Software.
  - 2.7 The Provider is responsible for maintaining up-to-date and accurate information with the Department (including a current e-mail address and other contact information required by the Department).
  - 2.8 The Department will not charge a fee for the Provider or Provider Personnel accessing the PRISMS API Services.
-

### 3. Use of the PRISMS API Services

- 3.1 The Provider must not, and the Provider must ensure that Provider Personnel do not, use the PRISMS API Services for any activity which:
- (a) constitutes a breach of any law;
  - (b) is prohibited by these Terms;
  - (c) is likely to cause loss or damage to any person, the PRISMS API Services or the Department's systems or data;
  - (d) transmits any viruses, worms, defects, Trojan horses, malware or any code of a destructive manner; or
  - (e) reverse engineers or attempts to extract source code from the PRISMS API.
- 3.2 The Provider must ensure that it complies, and that Provider Personnel comply, with the data security, privacy, system integrity and other requirements specified in the Provider Use Policy (as amended from time to time) that is made available on the PRISMS API Portal.
- 3.3 The Department may provide resources to the Provider in relation to the PRISMS API Services. The Provider acknowledges and agrees that the Department is not responsible for any loss or damage caused by any reliance on, or use made of, those resources by the Provider.
- 3.4 The Provider acknowledges that the Department monitors and collects information about all actual or attempted access to, and activity within, the PRISMS API. The Provider must provide any information requested by the Department in relation to its access to and use of the PRISMS API Services.
- 

### 4. Provider reporting obligations

- 4.1 The Provider acknowledges and agrees that:
- (a) it is responsible for the accuracy and timeliness of information that it reports to PRISMS through the PRISMS API;
  - (b) it will not be relieved of its reporting obligations under the ESOS Act in the event of a fault or outage of the PRISMS API Services which prevents the Provider from accessing or using the PRISMS API to enter information for the purposes of section 109 of the ESOS Act; and
  - (c) where the Provider is unable to access or use the PRISMS API to enter information for the purposes of section 109 of the ESOS Act, the PRISMS website (available at <https://prisms.education.gov.au>) or such other website as notified by the Department is available to the Provider to submit the information to PRISMS.
-

## 5. Privacy

- 5.1 The Provider must comply with all applicable privacy laws, including the Privacy Act.
- 5.2 The Provider must comply with, and ensure that Provider Personnel comply with, any privacy policy or guidelines notified to the Provider by the Department from time to time.
- 5.3 The Provider must immediately notify the Department if any of the following occur:
  - (a) the Provider receives a complaint from a third party (including a Vendor) about the handling of any Personal Information held or accessed by the Provider in connection with PRISMS or the PRISMS API Services;
  - (b) the Provider breaches its obligations under this clause 0 or becomes aware of circumstances that may reasonably suggest that it could have breached its obligations under this clause; or
  - (c) the Privacy Commissioner in any Australian jurisdiction requests information about or commences an investigation in relation to the PRISMS API Services.
- 5.4 The Provider must comply with any reasonable direction from the Department in connection with any potential or actual breach of privacy, including without limitation, unauthorised access to Personal Information in connection with the Provider's use of the PRISMS API Services.
- 5.5 If the Provider suspects that there may have been an Eligible Data Breach in relation to any Personal Information held by the Provider as a result of the Provider's access to the PRISMS API (including data retrieved via the PRISMS API), the Provider must:
  - (a) immediately report it to the Department and provide a written report within 3 days; and
  - (b) where requested by the Department, carry out an assessment in accordance with the requirements of the Privacy Act.
- 5.6 If the Provider is aware that there has been an Eligible Data Breach in relation to any Personal Information held by the Provider as a result of the Provider's access to the PRISMS API (including data retrieved via the PRISMS API), the Provider must:
  - (a) take all reasonable action to mitigate the risk of the Eligible Data Breach causing serious harm to any individual to whom the Personal Information relates;
  - (b) take all other action necessary to comply with the requirements of the Privacy Act; and
  - (c) take any other action as reasonably directed by the Department.
- 5.7 The Provider must ensure that all Provider Personnel who access or use Personal Information in connection with the API Services are informed about Provider's obligations under this clause 0.

---

## 6. Security and data protection

6.1 The Provider must:

- (a) implement safeguards to prevent unauthorised access, misuse, or corruption of data exchanged through the PRISMS API;
- (b) comply, and ensure Provider Personnel comply, with the Provider Use Policy as amended from time to time (available on the PRISMS API Portal) and any other directions or Department or Commonwealth policies as notified to the Provider from time to time;
- (c) maintain a Cyber Security Assessment Outcome of a suitable standard as determined by the Department to maintain access to the PRISMS API; and
- (d) undertake a Cyber Security Assessment every 3 years; and
- (e) on request of the Department, complete a new cyber security assessment questionnaire.

---

## 7. Technical Support

- 7.1 The PRISMS API Services and the PRISMS API Services Hub are provided on an 'as is' basis.
- 7.2 The Provider is responsible for entering into its own arrangements with Vendor(s) for the provision of technical support for the Applicable Recognised PRISMS-Integrated Software and the Provider's use of the PRISMS API.

---

## 8. Continuity of access

- 8.1 The Department provides the Provider with access to the PRISMS API Services on an "as is" and "as available" basis. The Department does not warrant that access to the PRISMS API Services by the Provider will be continuous or fault free. However, the Department will use reasonable endeavours to provide a consistent level of service.
- 8.2 The Provider acknowledges and agrees that if it is unable to access or use the PRISMS API to enter information for the purposes of section 109 of the ESOS Act, the PRISMS website (available at <https://prisms.education.gov.au> or such other website as notified by the Department) is available to the Provider to submit the information to PRISMS.
- 8.3 The Provider must promptly report to the Department:
  - (a) any loss of, or fault in, the Provider's access to the PRISMS API (unless the Department has issued a notification of a current PRISMS API outage); and

- (b) any event which compromises, may compromise, or may have compromised the security or integrity of the PRISMS API or the Department's servers, systems or networks providing the PRISMS API, or any of the Department's or a Provider's data.
  - 8.4 The Provider must provide all assistance reasonably requested by the Department to respond to and protect against a risk to the security or integrity of the PRISMS API Services and any of the Department's servers, systems, networks or data.
  - 8.5 The Department may modify or alter the PRISMS API at any time without notice, which may affect the Provider's access to the PRISMS API. However, the Department will endeavour to publish planned updates to the PRISMS API on the PRISMS API Portal.
- 

## 9. Circumstances to be notified to the Department

- 9.1 Without limiting the Provider's other obligations under these Terms, the Provider must promptly notify the Department if the Provider:
    - (a) experiences a Change in Control;
    - (b) becomes insolvent or comes under one of the forms of external administration referred to in chapter 5 of the *Corporations Act 2001* (Cth), or has an order made against it for the purpose of placing it under external administration;
    - (c) has been subject to a cybersecurity or data breach incident requiring reporting to the Australian Signals Directorate Australian Cybersecurity Incident Centre or the Office of the Australian Information Commissioner;
    - (d) is subject of investigation by a law enforcement or regulatory agency;
    - (e) becomes aware of a defect or fault in the Applicable Recognised PRISMS-Integrated Software, which is resulting in unintended behaviour in the PRISMS API; and
    - (f) wants to cease accessing the PRISMS API via any of the Applicable Recognised PRISMS-Integrated Software.
- 

## 10. Intellectual property

- 10.1 The Department grants the Provider a revocable, non-transferable, non-exclusive licence to use the PRISMS API:
  - (a) for so long as these Terms remain on foot and the Provider's access to the PRISMS API Services have not been suspended; and
  - (b) solely for the purpose of the Provider fulfilling its obligations under the ESOS Act.

- 10.2 The Provider does not acquire ownership of any rights in the PRISMS API Services or any of the data accessed by using the PRISMS API Services.
- 10.3 The Provider acknowledges and agrees that:
- (a) all data retrieved via the PRISMS API remains the property of the Department and the Provider's right to use or possess such data is granted solely for the purpose of fulfilling its obligations under the ESOS Act; and
  - (b) all intellectual property rights in data that the Provider provides through the PRISMS API (whether existing in a tangible or intangible form or format) will vest absolutely in the Department, and the Provider assigns all of its existing and future right, title and interest (including all intellectual property rights) in such data to the Department.
- 

## 11. Liability and indemnity

- 11.1 The Provider acknowledges and agrees that:
- (a) it uses the PRISMS API Services at its own risk; and
  - (b) to the extent permitted by law, the Department is not liable to the Provider or Provider Personnel for any loss or damage (however described) that is directly or indirectly related to:
    - (i) accessing or using the PRISMS API Services or the PRISMS API Services Hub; or
    - (ii) the unavailability or performance of any of the PRISMS API Services or the PRISMS API Services Hub.
- 11.2 The Provider agrees to indemnify the Department for any loss or damage (however described) suffered by the Department or a third party arising from or related to:
- (a) any breach of intellectual property rights by the Provider or Provider Personnel; or
  - (b) any breach by the Provider or the Provider Personnel of these Terms.
- 

## 12. Suspension and termination of access

- 12.1 The Department may by notice immediately suspend or terminate the Provider's access to some, or all, parts of the PRISMS API Services (including by disabling the Provider's Client IDs):
- (a) if the Department believes or suspects that the Provider has breached these Terms;
  - (b) the Provider is no longer registered with CRICOS;

- (c) the Provider no longer satisfies the eligibility criteria for access to the PRISMS API Services by education providers;
  - (d) if the Department believes or suspects that the Provider's access to the PRISMS API Services compromises, may compromise, or may have compromised the security or integrity of the PRISMS API Services or any of the Department's servers, systems, networks or data; or
  - (e) for any other reason.
- 12.2 The Department is not responsible for any loss caused by the suspension or termination of the Provider's access to the PRISMS API Services in accordance with these Terms, including any liability that the Provider has to a Vendor.
- 12.3 If the Department suspends the Provider's access to the PRISMS API Services under clause 0 the Provider must immediately stop using the PRISMS API Services (or that part of the PRISMS API Services for which access is suspended).
- 12.4 If the Department terminates the Provider's access to the PRISMS API Services:
- (a) the Provider must immediately stop using the PRISMS API Services (or that part of the PRISMS API Services for which access is terminated);
  - (b) unless otherwise specified in the termination notice, the Provider must immediately destroy all confidential information specified by the Department in the termination notice;
  - (c) the Department may audit the Provider to ensure it has undertaken all required actions set out in this clause 0.
- 12.5 The Provider may stop using the PRISMS API Services at any time by providing 28 days' notice to the Department.
- 12.6 If the Provider wants to terminate these Terms, the Provider must provide the Department with 28 days' prior written notice and upon termination, cease accessing or using the PRISMS API Services and ensure that Provider Personnel cease accessing or using the PRISMS API via the Applicable Recognised PRISMS-Integrated Software.
- 

## 13. Auditing

- 13.1 The Department may at any time without notice undertake an audit of the Provider's compliance with these Terms.
- 13.2 As part of any audit conducted under clause 0, where requested, the Provider must promptly (and within the timeframe requested by the Department) provide the Department with documentation regarding the Provider's use of any Applicable Recognised PRISMS-Integrated Software.

13.3 Failure by the Provider to comply with a request under clause 0 may result in the suspension or termination of the Provider's access to PRISMS API Services.

---

## 14. Governing law

14.1 These Terms are governed by the law in force in the Australian Capital Territory, Australia.

14.2 The Provider agrees to submit to the non-exclusive jurisdiction of the courts of the Australian Capital Territory, Australia in respect of any dispute under these Terms.

---

## 15. Execution

15.1 By signing the Provider agrees to be bound by these Terms.

### Provider Details

Provider Info	Details
Provider's legal name:	
Provider's ACN:	
Provider's ABN:	
Provider's email:	
Provider's postal address:	
Provider's representative:	

## EXECUTED as a DEED POLL

Option 1: Use this execution block if the Provider is a company incorporated under the Corporations Act.

Executed by *[insert full name and ABN of Provider]* in accordance with section 127 of the Corporations Act 2001 (Cth):

\_\_\_\_\_  
Signature of director

\_\_\_\_\_  
Full name of director

\_\_\_\_\_  
Full name of director

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of company secretary/director (print)

\_\_\_\_\_  
Full name of company secretary/director (print)

\_\_\_\_\_  
Full name of company secretary/director (print)

\_\_\_\_\_  
Date

Option 2: Use this execution block if the Provider is not a company incorporated under the Corporations Act.

Signed, sealed and delivered by *[insert full name and ABN (if applicable) of Provider]* in the presence of:

\_\_\_\_\_  
Signature of witness

\_\_\_\_\_  
Full name of witness (print)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of individual / authorised representative

\_\_\_\_\_  
Full name of individual / authorised representative (print)

\_\_\_\_\_  
Position of authorised representative (print)