UNIVERSITY FOREIGN INTERFERENCE TASKFORCE TRANSNATIONAL EDUCATION WORKING GROUP

TRANSNATIONAL EDUCATION CASE STUDIES

These case studies are intended to be read in conjunction with the Transnational Education Guidance Note on Due Diligence. They are designed to assist universities to understand how they might consider the Guidelines to Counter Foreign Interference in the Australian University Sector in the transnational education environment. The case studies are examples only. They provide a point of reference for decision makers to refer to as appropriate to their circumstances.

Case One – Due diligence: joint degree program/offshore campus

University X (the University) is considering entering into an arrangement with an international Institute of Tertiary Education (the Institute). The arrangement will likely commence with the delivery of a joint degree program, and will be a test for the University for the possible future establishment of a campus in that country. The arrangement would initially facilitate the delivery of courses in both Australia and overseas, for students from both countries. Courses would be taught both online and in-person at both campuses.

The University has a longstanding relationship with the Institute, and has been reciprocally sending students on exchange for a number of years with minimal incidents. However, in recent times, there has been an increase in the number of violent political protests and outbursts in some parts of the country, with Australian Government authorities advising Australians through the Smartraveller website to exercise a high degree of caution when travelling to this country.

The University has cybersecurity protections in place for students using its own systems and hardware. However, this proposed partnership would potentially involve Australian students studying at the Institute using the Institute's software systems. This would involve the Institute having access to the personal data of Australian-based students, irrespective of the University's protective security mechanisms. The University is aware that increased offshore data holdings and interaction may lead to increased cybersecurity vulnerabilities.

The University will need to consider these risks, among others, before deciding to partner with the Institute. The University would particularly like to ensure that if its overseas facilities face a cyber-attack or data breach, the personal data and research of its staff and/or students is secure. The University is

conscious of the possibility of foreign actors seeking to access this data to inappropriately interfere in their research direction or strategic interests.

The University's considerations should include:

- Consider the extend of personal security or safety risk present for staff and students, and to ensure staff and students know they can seek consular assistance from the Australian Embassy/High Commission if required.
- Consider pre-briefings or any staff or students travelling from Australia to the Institute to check the SmartTraveller website.
- The prospective operating environment and the legislative environment the campus would operate in – particularly in respect to in-country laws regarding privacy and data protection, and the jurisdiction which the partner university will operate within.
    - The University should assess these factors against its own policies and obligations under Australian law (such as the Australian Privacy Principles) to ensure any conflict is identified.
    - The University should also consider whether there is a need to disclose to students' information about who holds their data, in line with local laws and requirements.
- Its own, and the Institute's data storage, cybersecurity, and protective security risk management – whether both have implemented a cybersecurity strategy, informed by threat modelling, based on a best-practice controls framework – and whether extra measures need to be implemented to protect the data of Australian students.
    - This strategy should account for the offshore operating environment including rules and regulations in the host country. From this, the University should determine whether extra cybersecurity measures need to be implemented to protect the data of Australian students.
- Whether the country they are operating in has a history of cyber-attacks on universities, developing an understanding of incident management/process and previous responses.
- The nature and extent of any interoperability between the information systems of the Australian university and its international partner i.e. unauthorised access to data and/or information systems operated by the Australian university by the Institute as a result of the agreement (including by individuals sanctioned under Australian or United Nations Security Council sanctions frameworks).
- Whether the Australian university will have any reporting requirements, or other obligations under Australian law, as a result of its partnership with the Institute.
    - Has the University considered obligations under the Foreign Arrangements Scheme for any arrangement negotiated or entered into with the Institute?
    - Do the University and the Institute have processes in place to detect potential sanctions violations? Is a sanctions risk assessment required, and does the University need to apply for Australian sanctions or Defence Export Controls permits?
- If University X is a member of Defence Industry Security Program (DISP), consider any requirements that need to be met to remain compliant with DISP membership e.g. overseas travel briefings.
- Whether staff at the University and the Institute have been trained to understand sanctions policies, and how to detect and report non-compliance.
- Whether there are divergent expectations and practices around research collaboration between Australian and overseas researchers.

- Whether there are any intellectual property considerations around research undertaken at an overseas campus.

Case Two – Staff

An Australian academic at University Z (the University) teaches a number of science related undergraduate level courses, and supervises a number of PhD candidates in his field of specialisation – Quantum Physics.

The University has recently established a bricks and mortar campus overseas. The academic has been asked to lead the University's Faculty of Science at this new campus. In doing this, he will be required to frequently travel between Australia and the offshore campus.

While undertaking this role, the academic will still have supervision requirements for his PhD students located back in Australia, and will often have to review work and take meetings/calls with these students while travelling, including while in transit.

While travelling, he complies with the University's travel policy, ensuring risks associated with his frequent travel are considered and addressed – including the requirement to take a clean laptop (a laptop that does not contain any sensitive University data or access to protected University systems), a clean mobile phone, and not accessing any public or unrestricted internet/Wi-Fi services.

While on a routine overseas trip to the offshore campus, the academic takes a call from one of his PhD students in a public space on campus. The call with the PhD student involves a passing reference to sensitive research, linked to critical technologies that could have potential to impact Australia's national interests. After finishing the phone call, the academic is approached by a stranger who informs him that he is a researcher from a university in an overseas country (Overseas University), with an interest in the subject being discussed on the phone call. The researcher asks the Australian academic a number of questions about the research being undertaken and suggests to the academic that the Overseas University and the offshore campus of University Z could consider a research partnership on the subject.

The academic is aware that while international collaboration can lead to beneficial research outcomes and support bilateral relationships with partner countries, it also carries risks, especially in cases involving sensitive research. He thinks this could be a great opportunity for the University, but is concerned that the individual who approached him may have overheard sensitive details about the application of his research, and/or could use the partnership to access research material that should be protected in the national interest.

The academic should:

- Report the incident of the overheard phone conversation to the University Security team, both in Australia and in country, including raising the proposal for a research partnership
- Consider seeking consular assistance from the Australian Embassy/High Commission if he feels threatened by the approach.
- Pending the response from the University Security team about the incident, raise the proposed partnership with the appropriate area of the University to consider if a partnership is viable.

In its response, University Z should first consider:

- Whether a reportable incident has occurred under any information protection policies/laws.

- University Z should also consider whether further training on the handling and discussion of sensitive materials is required as part of the University's travel policy or pre-briefing.
- If the University Z security team establish that a reportable incident did not occur, and the academic, as lead of the University's Faculty of Science, decides to pursue the partnership, the University should:
    - Utilise the University's Due Diligence framework to consider the possible partnership and any risk of foreign interference.
    - Conduct a broad open-source search to identify any issues of concern regarding the operation of the Overseas University.
    - Consider how the Overseas University is governed, including its Council/Board, publicly available business or strategic plans, and its relationship to the government of the overseas country.
    - Consider engaging with trusted partners who interact or work with Overseas University to obtain reference as to their operations and reputation.

Case Three – Students

A PhD student at University W (the University) researches the correlation between education standards in western countries and the prevalence of modern slavery. She is already well respected in this subject, having published a number of works undertaken as part of a previous Masters course of study.

With her focus being on the Asia Pacific, the PhD student has a primary supervisor based at the University (Supervisor 1), as well as a secondary supervisor located at an international university (Supervisor 2) in the Asia Pacific region. This co-supervisor arrangement has been approved by the University. The PhD student has a good relationship with both supervisors, who have previously worked together academically, and been very considerate of one another's experiences and perspectives. Her co-supervisors have also consistently provided advice both collectively and individually.

Recently, Supervisor 2 has been consistently requesting the PhD student discuss and contribute to a number of other pieces of work with researchers based in a foreign country who she has not met or previously worked with. Supervisor 2 has been arranging a number of meetings without including Supervisor 1, sometimes challenging the PhD student's research and perspectives and providing a different interpretation of the work she has put forward. Conscious of diligently contributing to the work and to solidify her reputation, and aware of Supervisor 2's expertise on the subject matter, the PhD student has accepted most requests to contribute and Supervisor 2's changes to her work.

The PhD student's name and credentials are published as a contributor to these works, citing the University as her primary affiliation. However, she has not spoken to Supervisor 1 about her contributions to work beyond her PhD, and Supervisor 1 is also unaware of the extent of the PhD student's ongoing conversations with Supervisor 2.

Supervisor 1 is called into the office of the Deputy Vice-Chancellor, Research (DVCR). The DVCR has discovered that a number of international researchers who have also contributed to the work the PhD student is associated with are academics working for universities and organisations that have close ties with a foreign government. Engaging in this work and the non-disclosure of this collaboration and the extension of the PhD student's partnership with Supervisor 2 may be a breach of the University's Academic Misconduct Policy. The University is considering suspending her PhD candidacy.

In consider whether to suspend the PhD student, the University should consider:

- Whether appropriate due diligence was taken when assessing and approving the partnership between Supervisor 1 and Supervisor 2, with clear expectations on conduct and collaboration.
- Whether the PhD student's conduct was contrary to the University's declaration of interest policies and procedures – i.e. whether she was required to declare the invitation to collaborate with researchers overseas.
- Whether adequate training was provided to supervisors, research students and staff regarding the need to declare foreign affiliations and interests.
    - Whether clear and easily accessible staff and student academic integrity policies and procedures were provided by the University.
    - Whether academic integrity policies and procedures clearly relate to all students and staff.
- The reputational impact of a well-respected PhD student (and by extension, their supervisor) being associated an undisclosed partnership with a university without institutional autonomy.
- Whether the University has policies that cover the conduct of international academics undertaking a co-supervisory role, and their remit around the tasking of students.
- Whether the University has properly followed legislative compliance obligations and whether University staff understand the University's obligations under relevant government Schemes (such as the Foreign Arrangements Scheme).
- Whether the University has due diligence and compliance screening procedures in place to identify potential sanctions risks.