

FOREIGN INTERFERENCE POLICY AND PROCEDURE



CONTENTS

| | | |
|---|--|---|
| 1 | PURPOSE | 1 |
| 2 | SCOPE | 1 |
| 3 | POLICY STATEMENT | 2 |
| 4 | PROCEDURE | 3 |
| | Identifying the potential for foreign interference | 3 |
| | Education around foreign interference | 3 |
| | Due diligence with partnerships | 4 |
| | Reporting foreign interference..... | 4 |
| | Managing foreign interference arrangements | 4 |
| 5 | RESPONSIBILITIES | 4 |
| | Compliance, monitoring and review | 4 |
| | Reporting | 5 |
| | Records management..... | 5 |
| 6 | DEFINITIONS | 5 |
| | Terms and definitions..... | 5 |
| 7 | RELATED LEGISLATION AND DOCUMENTS | 7 |
| 8 | FEEDBACK | 7 |
| 9 | APPROVAL AND REVIEW DETAILS | 7 |

1 PURPOSE

- 1.1 This policy and procedure outlines how CQUniversity will manage [foreign interference](#) risk.

2 SCOPE

- 2.1 This policy and procedure applies to CQUniversity members, campuses (including transnational locations and operations), arrangements and locations involved or engaged in [foreign arrangements](#) or representing the University with a [foreign government](#), agency, corporation or individual including but not limited to:
- members of Council and Committees
 - employees, students and [affiliates](#)
 - employees and students of controlled entities of the University, and
 - physical and digital environments, research, teaching, infrastructure projects, financial investments, donations, travel, procurement, partnerships, third-party arrangements, agreement and contracts, joint ventures, memorandums of understanding, articulation agreements, University-controlled entities, employee and student recruitment activities and engagement activities.
- 2.2 Refer to the [Conflict of Interest Policy and Procedure](#) on how to manage conflicts of interest that fall outside the scope of this policy and procedure.
- 2.3 Refer to the [Cybersecurity Management Policy](#) for information on how the University will manage [cybersecurity](#) concerns, including those specifically related to [foreign interference](#), promote an international information security culture, information security risk management and response to threats on responsibilities to cybersecurity, promotion of an international information security culture and information security risk management and response to threats.

3 POLICY STATEMENT

- 3.1 All governments, including Australia's, try to influence deliberations on issues of importance to them. These [foreign influence](#) activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate.
- 3.2 Given it's at the leading edge of policy, research and scientific development though, Australia's university sector is one of the sectors at risk to [foreign interference](#). Most university international interactions are positive and benefit Australia; however, there are those who seek to interfere in the university sector (i.e. through inappropriately influencing course content, research directions, and student and employee actions).¹
- 3.3 Foreign interference can:
- damage the University's reputation
 - endanger employees' right to [academic freedom](#)
 - compromise the University's research, or other [sensitive or classified Information](#)
 - compromise partner organisation's confidence and support in the University
 - cultivate the University community for [espionage](#) against Australia, or
 - allow [foreign governments](#) to gain an undue commercial, technical or intellectual advantage to the disadvantage of the University.
- 3.4 Foreign interference can occur through:
- improper attempts to obtain sensitive or classified information from students or employees via foreign delegations, seminars and collaborations
 - targeting, compromising and recruiting employees and students to further a [foreign entity](#)'s interests
 - actions by, or for, a foreign entity that are inconsistent with academic freedom and the University's values, such as demands or inducements to change academic courses for the benefit of a foreign political, religious or social agenda
 - efforts to alter or direct the University's research agenda into particular areas of research (this may occur through subtle forms of [undue influence](#) and engagement, and through funding arrangements that may lead to a loss of future value and/or control of intellectual property)
 - seeking access to, or influence over, particular persons or areas of activity through various forms of funding arrangements (e.g. donations) or collaborations, [facilitation payments](#), or inducements targeted at individuals, or
 - cyber targeting by exploiting network vulnerabilities and unauthorised access.
- 3.5 By being aware of foreign interference risks, properly managing those risks, and applying appropriate security to sensitive or classified information and knowledge, the risk that such information might be used to advantage a foreign nation rather than Australia is reduced.
- 3.6 Australian citizens or permanent residents who are found to have failed to act to defend the national interest may be subject to disciplinary and/or criminal proceedings.
- 3.7 [University members](#) are subject to the Australian law, regardless of where an activity or action is undertaken. For example, if a bribe is given to a public official or if irregularities in financial accounting records are ignored or intended to conceal a bribe, there may be an investigation by the Australian Federal Police and criminal charges that can lead to imprisonment. This would also constitute corrupt conduct. The University has a zero tolerance for corrupt conduct. Further information on how to report suspected corrupt conduct, and how this will be investigated by the University is set out in the University's [Fraud and Corruption Control Framework](#) and [Public Interest Disclosure Policy and Procedure](#).
- 3.8 This policy and procedure aligns with the pillars and advice provided in the [Guidelines on Countering Foreign Interference in the Australian University Sector](#). These Guidelines provide an integrated approach for managing foreign interference risk under four pillars:

¹ [Guidelines to Counter Foreign Interference in the Australian University Sector](#)

- governance and risk frameworks
 - communications, education and knowledge sharing
 - [due diligence](#), risk assessments and management, and
 - [cybersecurity](#).
- 3.9 The University's compliance with the [Guidelines on Countering Foreign Interference in the Australian University Sector](#) will be undertaken by a Countering Foreign Interference Steering Committee, which will report to the Vice President (Research) as the University's [Accountable Authority](#).

4 PROCEDURE

Identifying the potential for foreign interference

- 4.1 Employees and Council members must complete the annual conflict of interest disclosure process, in accordance with the [Conflict of Interest Policy and Procedure](#). The Disclosure Statement Forms (for employees) and Declaration of Interest Questionnaire (for Council members) include specific questions that identify potential areas of [foreign interference](#).
- 4.2 This conflict of interest disclosure process will also be undertaken by new employees and Council members at the time of joining or becoming associated with the University.
- 4.3 Employees who self-identify through these questions as having potential exposure to foreign interference must undertake a mandatory training course that will be monitored for completion by supervisors, with guidance from the People and Culture Directorate and the Countering Foreign Interference Steering Committee.
- 4.4 Additionally, employees who wish to register a new partnership with an international organisation must complete a [due diligence](#) checklist before being able to register the partnership via the University's website (refer to the [due diligence with partnerships section](#) below).
- 4.5 Students (whether of the University or a University-controlled entity) will receive information about understanding and identifying potential foreign interference as part of their initial orientation materials, including directions to the University's [foreign interference webpage](#).

Education around foreign interference

- 4.6 Two training courses are available for employees:.
- The first is a general information package outlining the intent and detail of the [Guidelines for Countering Foreign Interference](#). This training course is optional, but is particularly valuable for senior University employees who wish to be informed of the high-level national security issues around [foreign interference](#).
 - The second is a training program which highlights the practical implications of foreign interference, and the specific University systems and processes for identifying and dealing with it. This training is required for employees who self-identify through the annual declarations process as being at risk of foreign interference, but will also optionally be available for all employees to access through the University's Corporate Learning Management System (EMPower).
 - Employees who wish to initiate a formal partnership agreement with an international organisation can access the University's [International Partnerships StaffNet Page](#) and relevant Gateway Document for information on how to complete the mandatory [due diligence](#) checks (refer to the [due diligence with partnerships section](#) below).
- 4.7 Commencing students will have a brief information sheet outlining the risks of foreign interference and how to identify it included in their orientation materials.
- 4.8 Messages will be distributed to students by the Student Communications Team and employees by the Corporate Communications Teams at the beginning of Term 1 and Term 2 each year as a reminder of the importance of being aware of the potential for foreign interference, and to direct people to the online resources on the University's [foreign interference webpage](#).

Due diligence with partnerships

- 4.9 The arrangements for forming foreign partnerships are available and explained on the University's internal [International Partnerships StaffNet page](#).
- 4.10 In accordance with the University's [Partnerships Policy and Procedure](#), employees wishing to enter into any kind of partnership arrangement (including mobility agreements and memoranda of understanding) with a [foreign entity](#), or with an organisation with links to a foreign entity, must complete the relevant [Gateway Document](#). Completion of the procedures outlined in the Gateway document is a requirement of formal approval and registration of any University partnership with an external entity.
- 4.11 As part of completing the [Gateway Document](#), proponents must undertake a [due diligence](#) process drawn from the Australian Security Intelligence Organisation (ASIO) Due Diligence Integrity Tool, available as a link in from within the Gateway document.
- 4.12 Additionally, the [Gateway Document](#) requires consideration in line with the [Australia's Foreign Relations \(State and Territory Arrangements\) Act 2020](#) (Cwlth) as to whether the partnership must be notified under the Department of Foreign Affairs and Trade [Foreign Arrangements Scheme](#). This Scheme provides an online portal for registering relevant [foreign arrangements](#), and provides of public register of such arrangements.
- 4.13 A Foreign Arrangements Scheme Decision Tool is available as part of the [Gateway Document](#), to assist in the decision around the need for [Foreign Arrangements Scheme](#) registration for a particular partnership.
- 4.14 Where prospective partnerships are identified through the [Foreign Arrangement Scheme](#) due diligence process as presenting potential [foreign interference](#) concerns, they will be referred to the Vice-President (Research) for endorsement, and to arrange for the registration of the partnership through the Foreign Arrangement Scheme portal.

Reporting foreign interference

- 4.15 Individuals who become aware of, or wish to raise issues associated with, [foreign interference](#) and the University can submit their concerns via:
- an anonymous notification form on the University's [foreign interference webpage](#), or
 - contacting the Chair of the Foreign Interference Steering Committee or Vice-President (Research).
- 4.16 Concerns will be investigated, determined and actioned by the Chair of the Foreign Interference Steering Committee (delegated by the Vice-President (Research)), in line with this policy and procedure, and the [Guidelines to Counter Foreign Interference in the Australian University Sector](#).

Managing foreign interference arrangements

- 4.17 The Countering Foreign Interference Steering Committee will be responsible for ensuring the actioning of this policy and procedure. Refer to the [Countering Foreign Interference Steering Committee Terms of Reference](#) for further information.

5 RESPONSIBILITIES

Compliance, monitoring and review

- 5.1 The Vice-President (Research), as the University's nominated [Accountable Authority](#), assisted by the Countering Foreign Interference Steering Committee, is responsible for:
- overseeing risk and reporting frameworks relating to [foreign interference](#), and implementing proportionate mitigation strategies that are effectively implemented and recorded
 - regularly reviewing and communicating security foreign interference risks and mitigations to the University
 - maintaining an awareness of [foreign arrangements](#), collaborations and funding entered into by the University, and ensuring that they have been assessed for risks associated with foreign interference

- overseeing University responses to reported issues about foreign interference
 - facilitating regular briefings on foreign interference risk management and issues to the University Council and its relevant Committees, and
 - implementing, monitoring, reviewing, and ensuring compliance with this policy and procedure.
- 5.2 The Countering Foreign Interference Steering Committee will conduct an annual review of foreign interference activities.

Reporting

- 5.3 The Countering Foreign Interference Steering Committee will present the Foreign Risk Register annually to Council via the Audit, Risk and Finance Committee and the University Management Committee.
- 5.4 The Vice-President (Research) will provide the Countering Foreign Interference Steering Committee's annual review of [foreign interference](#) activities to the University Management Committee for noting.

Records management

- 5.5 Employees must manage records in accordance with the [Records Management Policy and Procedure](#). This includes retaining these records in a recognised University recordkeeping information system.
- 5.6 University records must be retained for the minimum periods specified in the relevant [Retention and Disposal Schedule](#). Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

6 DEFINITIONS

- 6.1 Terms not defined in this document may be in the University [glossary](#).

Terms and definitions

Accountable authority: a member of the [Senior Executive](#) nominated by the Vice-Chancellor and President to hold ultimate responsibility for ensuring that University conforms to the [Guidelines for Countering Foreign Interference in the Australian University Sector](#).

Affiliate: a person (other than a member of the University Council or Committee, employee or student) who is affiliated with the University by letter of appointment or invitation to work, research or study for a particular activity, typically for a prescribed timeframe, and who is bound to comply with the University's policy documents during that period (for example, visiting scholars and adjunct appointees).

Cybersecurity: the technical and people capabilities, leadership, culture, techniques and practices that collectively protect an organisation's digital infrastructure and safeguard its data, systems and business operations against unauthorised access, attack, manipulation, disruption or damage.²

Due diligence: a process where reasonable steps are taken to obtain relevant information that will help reduce the risk of making an uninformed decision.²

Espionage: the theft of Australian information by someone either acting on behalf of a foreign power, or intending to provide information to a foreign power that is seeking advantage.²

Facilitation payments: payments made to officials with the intention of expediting an administrative process. The payment is meant to smooth the process of a service that the payer is legally entitled to. Facilitating payments are considered bribes and are prohibited by law.

Foreign arrangement: as per the [Foreign Arrangements Scheme](#) given effect through [Australia's Foreign Relations \(State and Territory Arrangements\) Act](#), any written arrangements, agreements, contracts, understandings or undertakings between State and Territory entities and foreign entities. They may be

² [Guidelines to Counter Foreign Interference in the Australian University Sector](#)

legally-binding or not legally-binding. This includes but is not limited to any of the following types of arrangements between the University and a foreign entity:

- foreign donations or investments
- international partnerships, memorandums of understanding, or articulation agreements
- employee fellowships or awards
- student exchange or study abroad agreements; research or service contracts, research collaboration agreements
- research grants, research grant applications that have been awarded by the funding body
- stipends, research higher degree entry arrangements, joint doctoral degree programs, and research scholarship agreements, and
- intellectual property commercialisation agreements; and international visit or study tour arrangements.

Foreign entity: defined under [Australia's Foreign Relations \(State and Territory Arrangements\) Act](#), foreign entity includes a foreign country, university without institutional autonomy, government, or department, agency or entity of a foreign government.

Foreign government: defined under [Australia's Foreign Relations \(State and Territory Arrangements\) Act](#), a foreign government includes a foreign national or sub-national government (including a department, agency or other public authority of that government). Some foreign tertiary education institutions, such as government military academies, would be considered part of the foreign government.

Foreign influence: governments, including Australia's, try to influence deliberations on issues of importance to them. These activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate.

Foreign interference: when activities carried out by, or on behalf of, a foreign actor, which are coercive, clandestine, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests.²

Foreign national: may include, but are not limited to, embassy or foreign government officials, including trade or business representatives.

Institutional autonomy: a foreign university does not have institutional autonomy when it is substantially under the control of a foreign government (including government or political appointees to the governing body), or its education, research or the academic employees are required by a law or the university's governing documents to adhere to political principles or doctrine. A foreign university's governing body may be referred to as the university council, committee, primary committee, senate, or board of trustees.

Universities with institutional autonomy separate from government, with freedom in relation to their internal governance, curriculum, research, teaching and discussion, and ability to publish those things, are not within scope of the [Australia's Foreign Relations \(State and Territory Arrangements\) Act](#).

Sensitive or classified information: official and confidential information created or managed by the University requiring protection from misuse or loss, which if eventuated, would harm the University's operational or strategic objectives.

Undue influence: when someone, because of their status or position, seeks or is able to derive an outcome that is favourable to them by exerting pressure over another person. That pressure is designed to get a member of the University to act in a way that is contrary to the University's best interests or their employment obligations, for example, to comply with University policy documents.

University members: a member of the University community which must adhere to this policy and procedure. University members include:

- members of the University Council and Committees
- employees, students and affiliates, and
- employees and students of controlled entities of the University.

7 RELATED LEGISLATION AND DOCUMENTS

- [Australia's Foreign Relations \(State and Territory Arrangements\) Act 2020](#) (Cwlth)
[Australia's Foreign Relations \(State and Territory Arrangements\) Rules 2020](#) (Cwlth)
[Autonomous Sanctions Act 2011](#) (Cwlth)
[Conflict of Interest Policy and Procedure](#)
[Countering Foreign Interference Steering Committee Terms of Reference](#)
[Countering Foreign Interference Webpage](#)
[Cybersecurity Management Policy](#)
[Defence Trades Control Act 2012](#) (Cwlth)
[Foreign Influence Transparency Scheme Act 2018](#) (Cwlth)
[Fraud and Corruption Control Framework](#)
[Guidelines to Counter Foreign Interference in the Australian University Sector](#)
[International Partnerships StaffNet Page](#)
[Partnerships Policy and Procedure](#)
[Public Interest Disclosure Policy and Procedure](#)

8 FEEDBACK

- 8.1 Feedback about this document can be emailed to policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

| Approval and Review | Details |
|------------------------------|---|
| Approval Authority | Council |
| Delegated Approval Authority | N/A |
| Advisory Committee | Audit, Risk and Finance Committee Countering Foreign Interference Steering Committee |
| Required Consultation | N/A |
| Administrator | Vice-President (Research) |
| Next Review Date | 13/03/2027 |

| Approval and Amendment History | Details |
|--------------------------------------|---|
| Original Approval Authority and Date | Audit, Risk and Finance Committee 13/03/2024 |
| Amendment Authority and Date | Editorial amendments 12/08/2024; Editorial amendments 03/10/2024. |
| Notes | |