Information and Privacy Policy and Procedures

Purpose

This Policy provides guidance on the Central Institute of Technology and Innovation's (the Institute) approach to its information handling practices in relation to the information collected from its students, staff, and others who interact with it. The Institute is committed to protecting personal privacy and recognises that staff and students have a reasonable expectation that the Institute will protect and appropriately manage the personal information it holds about them. The Institute where reasonably practicable is committed to the principles stipulated in the Privacy Act 1998 (Cth) (Privacy Act) and where the Institute has legislative and/or contractual obligations to the Commonwealth Government in circumstances as set out under Section 1.3 of this policy.

Scope

The policy applies to all staff, students, and other members of the Institute community to whom a policy applies.

Related Documents

This policy should be read in conjunction with the following Institute documents:

- Learning Management System Access and Support Policy and Procedures
- Acceptable Use of IT Policy and Procedures
- Conflict of Interest Policy and Procedures
- Code of Conduct Policy and Procedures

- Student Code of Conduct Policy and Procedures
- Intellectual Property Policy and Procedures

All documents referenced in this policy can be accessed via the CITI website.

Definition of Key Terms

For the purpose of this Policy, the following definitions apply:

Term	Definition
Disclosure	Disclosure means that the Institute makes personal information accessible to others outside the organisation and releases the subsequent handling of the information from its effective control.
System user	A system user is any Institute staff member, student, or external person who has been granted access to an Institute system for the purpose of work or study.
Consent	Consent, in this context, means any freely given, specific, informed and unambiguous indication where a system user or other individual signifies agreement to the processing of personal data and information relating to him or her.
Deliberate misuse	The wrong or improper use of Personal Information, done consciously and intentionally (on purpose). This includes unauthorised modification of data.
Inappropriate use	Inappropriate use means access to (and use of) personal information which is not appropriate to the individual's role or function at the time, for example, viewing the health records of an individual out of interest.
Privacy breach	Occurs when there is a failure to comply with this Policy. Usually, this will result in

Term	Definition
	unauthorised disclosure of or unauthorised access to personal information.
Notifiable breach	A notifiable data breach occurs if: • there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity. • the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates. • the entity has not been able to prevent the likely risk of serious harm with remedial action.
Personal information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Some examples are: • an individual's name, signature, address, phone number or date of birth. • sensitive information (see below) • financial or credit information • government identifiers e.g., passport number • photographs, video or voice recordings • internet protocol (IP) addresses • voice print and facial recognition biometrics • location information from a mobile device.
Sensitive information	Sensitive information is personal information relating to an individual's: • health

Term	Definition
	• racial or ethnic origin, including country of birth • political opinions • membership of a political association • religious beliefs or affiliations • philosophical beliefs • membership of a professional or trade association • membership of a trade union • sexual orientation or practices • criminal record • child related employment screening reports
Personal data	Personal data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of that natural person.
Privacy complaint	Is a complaint about an act or practice of the Institute in relation to an individual's personal information that is a breach of this Policy or Privacy Act.
Reasonably practicable	Reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure that a data breach does not occur, taking into account and weighing up all relevant matters.
Routine employment information	Is information that is solely and wholly related to the routine work duties and responsibilities of a staff member. This includes information such as a staff member's position title, JCU email address,

Term	Definition
	work phone number, professional opinion given in professional capacity, authorship of documents, incidental appearances of a staff members name in work documents, information about qualifications held, or any information which is publicly available on the JCU website.
Third party	A Third Party is an organisation, person, or other body, other than the Institute who is normally engaged by the Institute for the provision of a specified service.
Unauthorised access	Unauthorised access means obtaining and exercising access to personal Information, for which they are not authorised (by role or function) to access.

Policy Principles

The Institute strives to apply the Commonwealth Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) in its own practices to achieve consistency in protecting the privacy of individuals across the Institute. The Institute has established the following Information Privacy Framework to communicate the applicable privacy laws to staff, students, and others who interact with the Institute:

1. Incorporating the requirements set out in the Australian Privacy Principles into all relevant processes, procedures and systems.
2. Educating staff, students, Board and Committee members in the operation of this Policy.
3. Informing business partners, such as agents, internship providers, contractors and other professionals of these requirements with respect to information shared with them in the course of business.

4. Assuring all individuals interacting with the Institute that their personal information will be treated in accordance with this Policy.
5. Assuring all individuals interacting with the Institute that their personal circumstances at any given time will be treated in accordance with the Policy.
6. Providing secure means for the communication of personal information.
7. Providing mechanisms for the correction of personal information and for the lodging and handling of complaints about any suspected and/or notifiable breaches of this Policy.
8. Ensuring that no personal information is collected during access to the Institute's electronic communication platforms (e.g., website, email, social media, telephone calls) without the express consent of the user.
9. Ensuring that in applying this Policy that steps that are reasonably practicable have been applied to prevent unauthorised access, deliberate misuse, inappropriate use, and breaches in data protection.
10. These Principles regulate how: The Institute can collect, hold, use, and disclose personal and sensitive information. An individual can access and correct personal information or make a complaint about a suspected breach of the Policy.

Policy Statement

1. Collection and Use of Personal Information (Current and Prospective Students)

As part of its operations as a higher education provider, the Institute collects personal and sensitive information for lawful and reasonable purposes only and with the consent of the individual to whom the information relates. The Institute collects and uses personal and sensitive information from current and prospective students (and their parents/guardians if relevant) to:

1.1 Facilitate enrolment and progression through a course of study provided by the Institute.

1.2 Exercise its duty of care to foster and support student wellbeing and safety, including the effective resolution of complaints and grievances.

1.3 Build and maintain the Alumni community.

1.4 Meet legislative and/or regulatory record keeping or reporting requirements.

2. Collection and Use of Personal or Sensitive Information (Staff)

The Institute collects and uses personal and sensitive information from current and former staff to:

2.1 Support all aspects of the employee life cycle from recruitment to resignation/termination. This is considered to be routine employment information.

2.2 Exercise its duty of care to foster and support employee wellbeing and safety, including the effective resolution of complaints and grievances.

2.3 Meet legislative and/or regulatory record keeping or reporting requirements.

3. Collection and Use of Personal or Sensitive Information (Boards and Committees)

The Institute collects and uses personal and sensitive information from Board and Committee members to:

3.1 Support all aspects of the activities of all Boards and Committees.

3.2 Exercise its duty of care to foster and support wellbeing and safety of members, including the effective resolution of complaints and grievances.

3.3 Meet legislative and/or regulatory record keeping or reporting requirements.

4. Collection and Use of Personal or Sensitive Information (External)

The Institute collects and uses personal and sensitive information from *other* individuals external to the Institute where this is necessary to:

4.1 Enable the Institute to identify and interact with them if required during the course of Institute business, including the resolution of complaints.

4.2 Meet legislative and/or regulatory record keeping or reporting requirements.

5. Collection and Use of Unsolicited Personal Information

The Institute may receive unsolicited personal information. Such unsolicited information will only be collected and used from an individual if it is directly relevant to the Institute's primary purpose, such as the delivery of education programs to enrolled students, the well-being and safety of enrolled students, staff, and Board and Committee members and/or the resolution of complaints and/or grievances. The following may apply:

5.1 As part of these operational processes, the Institute may also become, or be made aware of, personal or sensitive information relating to external personal circumstances of an individual as a student, staff member or stakeholder.

5.2 In these cases, the Institute will take reasonable steps to ensure that the relevant individual/s is/are aware that their privacy is protected, both during and after the intervention and/or resolution process. Personal and/or sensitive information involved in such processes are/is collected and used in a manner that is also reasonably expected by the persons involved from a privacy perspective.

5.3 The Institute will notify the individual concerned when it collects personal and sensitive information either at the time of collection or as soon as practicable thereafter. This notification will also state:

5.3.1 What the personal and sensitive information will be used for and who will have access to it

5.3.2 Whether the provision of it is voluntary and the consequences for individuals if this personal and sensitive information is not provided, or only provided in part.

6. Use of Pseudonyms and/or Maintaining Anonymity

The Institute recognises that some individuals may wish to remain anonymous or use a pseudonym at some stages of their interactions with the Institute. Individuals will be notified where this is not reasonably practicable e.g., for enrolment, employment, or grievance resolution.

7. Storage and Security of Personal or Sensitive Information

Access to personal and sensitive information held by the Institute is restricted to authorised persons who are staff members, contractors, business partner representatives or other professionals who require such access to perform their duties

for the Institute. The Institute will take reasonable steps to ensure that its holdings of personal and sensitive information are:

7.1 Protected from loss, unauthorised access, use, modification, or other misuse.

7.2 Disposed of lawfully and securely.

7.3 Kept securely and for no longer than is necessary.

7.4 Accurate, up to date, complete, and not misleading.

7.5 Relevant to the Institute business.

7.6 Not excessive or unreasonably intrusive.

8. Disclosure of Personal or Sensitive Information

The Institute will not disclose personal or sensitive information to third parties outside of the core business of the Institute unless the Institute:

8.1 Has a duty of care to disclose this information to the Police and a parent/guardian of a student or visitor under the age of 18.

8.2 Is required to do so by legislation, court order or other legally enforceable instrument received in appropriate written form.

8.2.1 Reasonably believes disclosure to be necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.

8.2.2 Has the written consent of the individual concerned.

8.2.3 Will ensure that business partners (local or overseas), such as agents, internship providers, contractors and cloud computing providers are made aware of these requirements with respect to information shared with them in the course of business. The Institute will deal promptly with any unauthorised disclosures of personal information.

9. Access to and Correction of Personal and Sensitive Information (Current and Prospective Students)

Current and Prospective Students may seek access and request corrections to the personal and sensitive information collected about them by contacting the Institute. Access may be denied if such access would have an unreasonable impact on the privacy of others, or where such access may result in a breach of the Institute's duty of care to the student concerned. Authorised corrections will be made as soon as practicable and without charge.

10. Access to and Correction of Personal and Sensitive Information (Staff and Board/Committee Members)

Staff and Board/Committee members may seek access and request corrections to the personal and sensitive information collected about them by contacting Human Resources. Access may be denied if such access would have an unreasonable impact on the privacy of others, or where such access may result in a breach of the Institute's duty of care to the staff member concerned. Authorised corrections will be made as soon as practicable.

11. Access to Personal and Sensitive Information (External)

Other individuals external to the Institute may contact the Institute via the Institute website and will be advised within ten (10) working days of receiving this written request of how they may access or obtain a copy of their personal information, and any applicable processing fees.

12. Complaints and other Privacy Enquiries

Complaints about privacy breaches by the Institute are handled in accordance with this Policy. If an individual has a complaint or other privacy enquiry about how their personal or sensitive information is collected, held, used, secured, or disclosed should lodge an application for internal review in the first instance by writing to the Institute via the Institute's website.

Procedures

1. Application for an Internal Review

Any student, staff member, or board/committee member who believes the Institute has misused their personal or sensitive information can lodge an application for an internal review. The Institute will conduct an internal review to determine:

1.1 Whether or not the alleged conduct occurred

1.2 If so, whether the Institute complied with its privacy obligations

1.3 If not, whether non-compliance was authorised by an exemption, Privacy Codes of Practice, a direction from the Chief Executive Officer or delegate, or an appropriate action by way of a response/remedy Once it completes its internal review, the Institute will advise the relevant parties of the findings and the steps to address the findings.

2. Time Limit for Internal Review

The request for an internal review must be made within 6 months of the time of the event. The student, staff member, or board/committee member should raise the complaint as soon as they become aware of:

2.1 The conduct, the subject of the complaint.

2.2 Their rights under the Privacy legislation

3. The Internal Review Process

Applications for internal review must be made in writing by completing an online form that is accessed via the Institute website.

3.1 When the Institute receives the written application for internal review, the Chief Executive Officer (or delegate) will appoint a staff member to undertake the review. This will be a person who was not substantially involved in any matter relating to the conduct which gave rise to the complaint and who is otherwise suitably qualified to deal with the matters raised in the application.

3.2 The internal review will include interviews with key parties involved or identified in the application.

3.3 The internal review will include consideration of all relevant material submitted by the applicant, information obtained through interviews with relevant individuals, information obtained from the Institute's information and recordkeeping systems, policies and procedures or other relevant documents, and relevant legislation and standards.

4. The Outcome of the Internal Review Process

The outcomes of an internal review may include one or more of the following findings:

4.1 Insufficient evidence to prove alleged conduct occurred.

4.2 Alleged conduct did not occur, therefore no further action to be taken.

4.3 Alleged conduct occurred but complied with the relevant policies and legislation.

4.4 Alleged conduct occurred, conduct did not comply with the relevant policies and legislation but that the non-compliance was authorised.

4.5 Alleged conduct occurred, conduct did not comply with the relevant policies and legislation but that the non-compliance was not authorised.

4.6 Review/change in policies, practices or system controls to prevent the recurrence of a breach, or to undertake actions to prevent the conduct from recurring.

4.7 A formal apology to the applicant.

4.8 Training for staff

4.9 Appropriate remedial action as deemed appropriate by the Institute.

4.10 Any relevant undertakings to ensure that the conduct will not occur again.

5. Notification of Internal Review/Outcome

The final report including any findings and/or recommendations will be submitted to the Board of Directors for approval. The approved report will be sent to the complainant. The following points apply:

5.1 Where practicable, the review process will be concluded within 60 days of receiving the application for internal review.

5.2 If the review is not completed within 60 days from the date the application was received, then the complainant has 28 days to make an application under section 55 to the NSW Civil and Administrative Tribunal (NCAT) for a review of the conduct or decision complained about.

5.3 If the internal review is finalised after 60 days, then the complainant will have 28 days from the date they were notified of the result of the internal review to go to the Tribunal.

6. Application for an External Review

The only external review mechanism available under the Privacy and Personal Information and Protection Act (2012) is the right to apply for an administrative review of the conduct or decision complained about to the NSW Civil and Administrative Tribunal (NCAT) when:

6.1 An applicant is dissatisfied with the findings of an internal review; or

6.2 The Institute has not completed an internal review within 60 days of the application date.

Related Legislation

This policy should be read in conjunction with the following related documents:

- Higher Education Standards Framework (Threshold Standards) 2021
- Education Services for Overseas Students Act 2000
- Copyright Act 1968
- Anti-Discrimination Act 1977
- Privacy and Personal Information Protection Act 1988
- Criminal Code Act 1995
- Privacy Amendment (Private Sector) Bill 2000 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Bill 2021 (Cth)
- Australian Privacy Principles (2014) (Cth)
- Health Records Information and Privacy Regulation (NSW) 2012
- NSW Civil & Administrative Tribunal

Change and Version Control

Version	Date Approved	Authored by	Approved by	Description
1.0	29/09/2023	Chief Executive Officer	Board of Directors	Corporate Policy

Policy Information

Author	Chief Executive Officer
Responsible Officer	Chief Executive Officer
Approved by	Board of Directors
Approval date	29/09/2023
Status	Approved (Current Version)
Next review due	29/09/2026

Name of Policy	Information and Privacy Policy and Procedures	
Version	V1.0	
Policy: **Corporate**	Date: 29/09/2023	Status: Final ratified by the Board of Directors on 29/09/2023

File: Information and Privacy Policy and Procedures_V1.0