PRIVACY POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure ensures that personal information of students, employees, contractors, and members of the public collected and held by CQUniversity is accessed, used and disclosed in line with legislative requirements.

2 SCOPE

2.1 This policy and procedure applies to CQUniversity employees and individuals acting as the University's agents (including any controlled entities, contractors, consultants, and volunteers).

3 POLICY STATEMENT

3.1 As a statutory authority, CQUniversity must comply with the *Information Privacy Act 2009* (Qld) which aims to safeguard the handling of an individual's personal information in public sector environments.

3.2 CQUniversity's core functions require the collection, use and disclosure of personal information about students, employees and other individuals. The University is committed to protecting privacy and recognises that communities and stakeholders have a reasonable expectation that the University will protect and appropriately manage the personal information in its possession.

4 PROCEDURE

Collection of personal information

4.1 Personal information must be collected only where necessary and relevant to the University's functions and activities. Refer to the University's privacy website for examples of personal information held.

4.2 When information is collected directly from an individual, employees must tell the individual what the information is going to be used for before, or at, the point of collection where possible. If this is not possible, these details must be provided as soon as practicable after the information is collected.

4.3 Personal information must be obtained in a reasonable and transparent way. The University will not collect information by unlawful or unfair means, including trickery, deception, or misleading conduct.

4.4 The University may in certain circumstances transfer personal information overseas. Where the University transfers personal information overseas, it will comply with the provisions of the *Information Privacy Act* that relates to transborder data flows. The University will take all reasonable steps to ensure third party service providers do not use or disclose transferred personal information for a purpose other than for which it was collected.

Collection notices

4.5 Before collection, or as soon as practicable afterwards, the University must inform the individual from whom personal information is collected of:

- the purpose of collecting the information
- the law that authorises collection, namely the *Information Privacy Act,* and
- to whom the University normally discloses the information, and if known, anyone they in turn will disclose to.

4.6 This is usually provided in the form of a Collection Notice. Sample Collection Notices for employee use are provided on the Collection Notice Information Sheet located on the Privacy StaffNet page.

Consent

4.7 Consent is central to privacy, which revolves around the individuals' control over and knowledge about what is being done with their personal information.

4.8 Further consent is required for the collection, use, and disclosure of personal information, for a purpose other than the purpose for which it was collected.

4.9 Consent must be:

- Informed:
  - the University must explain how personal information will be handled, and
  - the explanation must be in plain English without legal or industry jargon/abbreviations.
- Voluntary:
  - the University must not force or pressure an individual to give consent.
- Current and specific:
  - the University must explain the reason for the request, being as specific as possible.

4.10 The individual providing consent must have capacity to give consent. Capacity means the individual:

- understands what is being asked
- understands the consequence of giving or not giving consent
- bases a decision on reason, and

- can communicate their decision.

4.11 Due to minors' status as vulnerable persons, the consent of a parent or guardian is required before the collection, use, or disclosure of their personal information. The exception to this is where the minor is a CQUniversity student, and the proposed collection, use, or disclosure directly relates to their education.

4.12 Common situations where individuals may not be able to give consent include:

- there is a physical or mental disability
- temporary incapacitation, and
- they have a limited understanding of English.

4.13 If the University is unsure if an individual has the capacity to give consent, support must be offered. If support is insufficient, the University may consider if someone can act on the individual's behalf, such as:

- a guardian
- someone with enduring power of attorney
- a person recognised by other relevant laws, or
- a person the individual nominated in writing when they were capable of giving consent.

As far as practicable, the University will involve the individual who lacks capacity in the consent decision.

4.14 All matters relating to capacity will be directed to the Legal Office (legaladvice@cqu.edu.au) for advice.

Express consent

4.15 Express consent is given openly, verbally or in writing (e.g. signing your name, by hand or by an electronic or voice signature).

Withdrawal of consent

4.16 Consent can be withdrawn at any time. The University must ensure the individual understands the possible consequences of withdrawing consent (e.g. the individual may no longer have access to a service).

4.17 Once consent has been withdrawn, the University will not rely on past consent for any future use or disclosure of personal information.

Photographs and video recordings

4.18 Employees taking photographs or recordings must obtain express consent from the individual if:

- an individual is clearly identifiable in the image/recording, and
- the image/recording will be made available for University purposes, including University publications, webpages, displays, and presentations.

4.19 A Talent Release Form must be completed prior to use of any photographic image or recording. The form may be completed after the image/recording has been taken, but the image/recording must not be used for University purposes if the individuals declines to provide consent. Completed Talent Release Forms must be kept by the business area in accordance with the General Retention and Disposal Schedule.

Relevance of personal information

4.20 Each Division and Directorate must be satisfied that the specific purpose for which they are collecting personal information relates to the functions of the University.

Storage and security of personal information

4.21 The University will take reasonable steps to protect personal information from misuse, loss and unauthorised access, modification, or disclosure.

4.22 The level of storage and security will depend upon the nature of the personal information recorded and the risk of a security breach occurring. If a document contains extremely sensitive information, such as health records, the University must take maximum care in protecting the information.

4.23 The Information Assets Security Classification Policy provides further details on how to classify and protect personal information.

Employee privacy

4.24 Employees must respect the privacy of other employees concerning their personal circumstances and illnesses. Personal information (even if affecting work) may not be disclosed unless necessary for the administration of emergency health care (e.g. providing to paramedics).

Access to personal information

4.25 Access to personal information will only be granted where necessary for work purposes. Employees must only access personal information for a work-related purpose.

4.26 Access to personal information for research purposes may be granted for planning and delivery improvements of core services offered by the University.

4.27 Access to personal information by utilising learning analytics may be granted for:

- prompts or suggestions sent to students via emails to their University email account, and
- employees contacting individual students if the University considers the student may benefit from additional support.

4.28 Contractual arrangements entered by the University may require third parties to have access to or use personal information owned or held by the University. Any contract entered by the University must include appropriate safeguards for protecting personal information.

4.29 The *Information Privacy Act* provides individuals the right to request access to the personal information which the University holds about them. Individuals requesting access to their own personal information can do so by completing a Right to Information and Information Privacy Access Application (RTI application form) and emailing it to privacyrti@cqu.edu.au or posting it to:

Coordinator Records and Privacy
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

External requests for personal information

4.30 External requests for personal information must be made in writing, and emailed to privacyrti@cqu.edu.au or posted to:

Coordinator Records and Privacy
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

Requests will be reviewed and escalated to the Legal Office where required.

Requests for personal information made by telephone

4.31 Where a request for information is made by telephone, employees will not release any information, as the identification of the caller is unable to be verified. The employee must ask the requester to send a request in writing and the request will be managed in accordance with section 4.30 above.

Requests for personal information made by police or other investigating officers

4.32 In all instances where police or other investigating officers enter a University campus to make enquiries, seek records or request assistance in an investigation, employees must contact the Director Governance or Coordinator Records and Privacy immediately.

4.33 In all other instances where the request for assistance is made in writing or by telephone, the police officer or investigating officers must be directed to the Records and Privacy Team (via privacyrti@cqu.edu.au) before any assistance is provided.

4.34 This policy and procedure does not intend to circumvent the existing operational procedures in place where the University's contracted Security Officers and Crisis Management Control Group contact the police in the case of reporting a crime or any other serious incident on any campus of the University.

Requests for personal information of a deceased person

4.35 The University must provide the same respect and level of protection for personal information of deceased students, alumni and employees. Requests for personal information of a deceased person must be made in accordance with the *Right to Information Act 2009* (Qld) and can be done so by completing a Right to Information and Information Privacy Access Application (RTI application form) and emailing it to privacyrti@cqu.edu.au or posting it to:

Coordinator Records and Privacy
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

Amendment of documents containing personal information

4.36 The *Information Privacy Act* provides individuals the right to amend personal information held by the University if they believe the information is inaccurate, incomplete, out of date or misleading. Individuals requesting amendments to their own personal information can do so by completing a valid Information Privacy Personal Information Amendment Application. Applications can be emailed to privacyrti@cqu.edu.au or posted to:

Coordinator Records and Privacy
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

Accuracy of personal information

4.37 Before using personal information, employees must take all reasonable steps to ensure the information is accurate, up-to-date, and complete.

Use of personal information

4.38 The University must only use personal information that is directly relevant to fulfilling the particular purpose for which it was provided.

Limits on disclosure of personal information

4.39 Employees must not disclosure personal information to individuals or organisations outside of the University.

4.40 In limited circumstances, personal information may be disclosed without breaching personal privacy. These circumstances include:

- appropriate documentary evidence demonstrating an individual has agreed to disclosure

- a privacy notice was given at the point of collection advising the individual about the usual practices for disclosure
- disclosure is required or authorised by law (e.g. court order, subpoena or a legislative obligation to disclose), or
- disclosure is necessary for investigation or enforcement of criminal matters or other law enforcement matters.

Privacy complaints

4.41 Individuals who believe the University has not dealt with their personal information in accordance with the *Information Privacy Act* or this policy and procedure, may make a formal privacy complaint.

4.42 A formal privacy complaint must be made in writing to the Coordinator Records and Privacy or referred to that officer if received by another area of the University. Privacy complaints can be emailed to privacyrti@cqu.edu.au or posted to:

Coordinator Records and Privacy
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

4.43 A formal privacy complaint must:

- include an address of the complainant
- give details about how their privacy is alleged to be breached, and
- be made within 12 months of the occurrence of the alleged breach.

4.44 Privacy complaints that are made more than 12 months after the occurrence of the alleged breach may not be able to be investigated, due to the difficulty in obtaining reliable evidence because of the length of time that has passed.

Refusal to deal with the complaint

4.45 A privacy complaint may be refused when:

- the complaint does not concern the personal information of the complainant
- the complaint concerns the personal information of a child and the person making the complaint is not the parent or guardian of the child
- the complaint concerns the personal information of an individual and the person lodging the complaint is not an agent of the individual authorised to act on the individual's behalf, or
- 12 months has elapsed since the complainant first became aware of the act or practice that is the subject of the complaint.

Acknowledgement

4.46 Privacy complaints will be acknowledged within five working days from the date the complaint is received.

4.47 Throughout the review and investigation of the privacy complaint, the complainant will be updated as appropriate.

Investigating a privacy complaint

4.48 Privacy complaints will be investigated by the Director Governance (or delegate) or the Legal Office, depending on the nature and complexity of the complaint.

4.49 The timeline for investigating and deciding a complaint will vary depending on the nature and complexity of the complaint.

4.50 Where a privacy complaint could have an adverse impact, the Director Governance (or delegate) or the Legal Office will consider whether it is appropriate to notify any affected individuals.

4.51 The Director Governance (or delegate) or the Legal Office, will consider whether it is appropriate to notify the Information Commissioner.

Complaint outcomes

4.52 Complainants will be provided with a written response to their complaint advising permissible findings of the investigation and any actions identified.

4.53 If the investigator of the privacy complaint is satisfied that the alleged breach occurred, resolution outcomes may include one or more of the following:

- an apology to the complainant
- a change to work responsibilities, work practices, or policies and procedures
- an explanation of how and why the problem occurred and what steps will be taken to prevent it from reoccurring, or
- disciplinary action under the University's Enterprise Agreement.

Internal review requests

4.54 Individuals who are not satisfied with the outcome of the privacy complaint may seek an internal review. A request for internal review must be lodged by the complainant within 20 working days of the date of the written outcome of their privacy complaint. If there are exceptional circumstances that prevented the internal review request being not lodged within 20 working days, the request for an internal review should provide details and evidence of the exceptional circumstances. Requests can be emailed to privacyrti@cqu.edu.au or posted to:

Director Governance
Governance
CQUniversity Australia
554 – 700 Yaamba Road
NORMAN GARDENS QLD 4701

4.55 If the Director Governance has previously been involved in the matter to be reviewed, the Chief Operating Officer (or delegate) will conduct the internal review.

4.56 Internal review requests will be acknowledged within five working days from the date the request is received.

4.57 The timeline for investigating and deciding an internal review will vary depending on the nature and complexity of the complaint.

4.58 Throughout the internal review, the complainant will be updated as appropriate.

4.59 Complainants will be provided with a written response to their request for an internal review advising permissible findings of the review and any actions identified.

External review request

4.60 Applicants who are dissatisfied with the outcome of the their privacy complaint or the University's internal review of their complaint outcome may apply in writing to the Office of the Information Commissioner for an external review. It is not necessary to have an internal review before applying for an external review.

4.61 External review requests must be made in writing to the Office of the Information Commissioner within 20 business days of the complaint outcome or the internal review outcome (whichever is later).

4.62 A request for an external review can be lodged in one of the following ways:

In person: Level 7, 133 Mary Street, Brisbane
Post: PO Box 10143, Adelaide Street, BRISBANE QLD 4000
Email: administration@oic.qld.gov.au
Online: https://www.oic.qld.gov.au

Further action

4.63 If the complaint cannot be resolved through the external review by the Information Commissioner, the complainant may ask the Information Commissioner to refer the matter to the Queensland Civil and Administrative Tribunal (QCAT).

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 For the purposes of the *Information Privacy Act*, the Vice-Chancellor and President, as the Chief Executive Officer of the University, is the 'principal officer' and, as such, is the person responsible for the University's obligations under the *Information Privacy Act*.

5.2 The Director Governance administers the *Information Privacy Act,* and has general responsibility for privacy management across the University, including:

- training employees in the University's privacy obligations
- providing advice on privacy issues
- assisting in developing privacy notices, and
- coordinating the University's investigation and response to privacy complaints.

5.3 Heads of business areas are responsible for assessing privacy risks in their area of responsibility, and for implementing business processes consistent with the Information Privacy Principles contained in the *Information Privacy Act*. Specific, ongoing responsibilities include:

- implementing and regularly reviewing appropriate data collection practices
- ensuring personal information is used, managed, and disclosed appropriately by employees within the business area and administrative practices are consistent with the University's privacy obligations
- implementing adequate security requirements for access to and storage of personal information in all formats within the business area, and
- ensuring privacy awareness is embedded in practices and procedures of the business area as appropriate.

5.4 The Director Governance is responsible for implementing, monitoring, reviewing and ensuring compliance with this policy and procedure. Compliance is monitored through scheduled audits and exception reporting.

Reporting

5.5 Annual reports on access applications processed under the *Information Privacy Act* and the *Right to Information Act* are provided to the Department of Justice and Attorney-General. The Coordinator Records and Privacy is responsible for compiling and providing these reports.

Records management

5.6 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.

5.7 University records must be retained for the minimum periods specified in the University Sector Retention and Disposal Schedule on the Queensland State Archives website. Before disposing of any records, approval must be sought through the Records Management Office (email records@cqu.edu.au).

6 DEFINITIONS

Terms not defined in this document may be in the University glossary.

Terms and definitions

Disclosure: release of personal information to another entity (e.g. a body, agency or person separate from the University) where the University will cease to have effective control of the personal information once it is released.

Information: any collection of data that is processed, analysed, interpreted, classified, or communicated in order to serve a useful purpose or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, and textual or numerical form.

Personal information: defined in the *Information Privacy Act* as "information or an opinion including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

It is not necessary for the information to be sensitive or confidential. It is also not necessary for the information to directly disclose the identity of an individual. It is sufficient that their identity could be ascertained through a series of steps, for example, by combining several pieces of information".

What is not personal information: Schedule 1 to the *Information Privacy Act* sets out categories of documents to which the Information Privacy Principles (IPPs) do not apply to the extent that those documents contain personal information. These include documents concerning:

- certain complaints and investigation of misconduct under the *Police Service Administration Act 1990* (Qld) and the *Crime and Corruption Act 2001* (Qld), and
- public interest disclosures made under the *Public Interest Disclosure Act 2010* (Qld).

Sensitive information: a type of personal information which may result in discrimination or harm if it is mishandled. Examples of sensitive information include:

- race or ethnic origin
- religious beliefs
- membership of professional associations or trade unions
- sexual preference
- health information, and
- criminal records.

7 RELATED LEGISLATION AND DOCUMENTS

Central Queensland University Enterprise Agreement 2017

Collection Notices Information Sheet (StaffNet)

Contract Management Policy and Procedure

Cybersecurity Management Policy

Data Breach Management (StaffNet)

Information Assets Security Classification Policy

Information Privacy Act 2009 (Qld)

Information Privacy Personal Information Amendment Application

Legal Services Policy

Partnerships Policy and Procedure

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cwlth)

Right to Information Act 2009 (Qld)

Right to Information and Information Privacy Access Application

Records Management 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	Vice-Chancellor and President
Delegated Approval Authority	Chief Operating Officer
Advisory Committee	N/A
Required Consultation	N/A
Administrator	Director Governance
Next Review Date	23/04/2024

Approval and Amendment History	Details
Original Approval Authority and Date	Vice-President (Student and Corporate Services) 23/04/2021
Amendment Authority and Date	Vice-President (Student and Corporate Services) 24/08/2022; Editorial amendment 03/01/2023.
Notes	This document replaced the Information Privacy Policy and Procedure (23/04/2021).