INFORMATION PRIVACY POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 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 the public sector environment, and provides for:

- the fair collection and handling of personal information by CQUniversity, and
- a right of access to, and amendment of, personal information in CQUniversity's control, unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended.

1.2 The *Information Privacy Act* specifies 11 Information Privacy Principles (IPPs) with which the University must comply. These govern how and when personal information may be collected, handled, stored, accessed, amended, managed, transferred, used and disclosed.

2 SCOPE

2.1 This policy and procedure applies to the collection of personal information, regardless of when it came into existence, and to the storage, handling, accessing, amendment, management, transfer, use and disclosure of personal information regardless of when it was collected.

2.2 This policy and procedure applies to all staff of the University, and provides information for all staff, students and the community in general.

3 POLICY STATEMENT

3.1 CQUniversity's functions require the collection, creation and use of personal information about students, staff and other individuals. CQUniversity is committed to protecting personal 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 and use of personal information

4.1 Personal information must be collected only where necessary and relevant to CQUniversity's functions and activities and in a reasonable and transparent way. Personal information should not be collected unless there is a specific and immediate use for it. An appropriate privacy notice must be provided when collecting information directly from an individual

4.2 Before using personal information, staff have a responsibility to take reasonable steps to ensure that information is accurate, up-to-date and complete. Personal information must be used only when it is relevant and only for the purpose for which it has been collected or a directly related purpose.

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

Access and security for personal information records

4.4 Access and security safeguards are important ways of protecting personal privacy. Access to personal information is granted to staff only where this is necessary for work purposes and staff must only access personal information if there is a work related reason for this. Personal information must be protected against loss, unauthorised access or modification, disclosure or misuse. The University's Information Security Management Policy and Procedure (FMPM) provides further details on how to classify and protect personal information.

Prohibition on disclosure of personal information

4.5 Staff must not disclose personal information to individuals or organisations outside the University. Disclosure refers to release of personal information to another entity (e.g. a body, agency or person separate from the University) where CQUniversity will cease to have effective control of the information once it is released, and

4.6 There are some limited circumstances in which personal information may be disclosed without breaching personal privacy. These circumstances include the following:

- where there is appropriate documentary evidence that individual has agreed to disclosure
- where a privacy notice given at the point of collection advises the individual about the usual practices for disclosure
- where disclosure is required or authorised by law (for example, court order or subpoena, legislative obligation to disclose)

- where disclosure is necessary to manage or lessen a serious threat to a person's life, health, safety or welfare, or to public health, safety or welfare, and/or
- where disclosure is necessary for investigation or enforcement of criminal matters or other law enforcement matters.

4.7 CQUniversity, including its predecessor institutions, maintains a public register of graduates. Information concerning a person's status as a graduate is a matter of public record and available to any member of the public upon formal request to the Director, Governance. The only details confirmed through this service are the graduate's name, the degree conferred or to be conferred and the date of conferral. CQUniversity may charge a fee for this service.

Access to personal information and rights to amendment

4.8 The *Information Privacy Act* gives an individual the right to request access to the personal information which the University holds about them, and to amend it where it is inaccurate, incomplete, out-of-date or misleading, except if this is not permitted by law

4.9 Individuals requesting access to their own personal information can do so by completing a valid Right to Information and Information Privacy Access Application Form and emailing it to privacyrti@cqu.edu.au or posting it to:

Privacy and Right to Information Officer
Governance Directorate
CQUniversity Australia
ROCKHAMPTON QLD 4701

Privacy complaints

4.10 If an individual believes that CQUniversity has not dealt with their personal information in accordance with the *Information Privacy Act 2009* or this policy, they may make a complaint to CQUniversity. A complaint must be made in writing or by email to the Manager, Corporate Governance or referred to that officer if received by another area of the University.

4.11 The Manager, Corporate Governance will refer the matter to the head of the organisational unit to resolve the complaint.

4.12 Primary responsibility for investigating and responding to the complaint will rest with the head of the relevant unit, with advice from the Manager, Corporate Governance as required. The University's main objective in responding to privacy complaints is to conciliate an outcome which is acceptable to the complainant and which addresses any broader or systemic privacy issues which may arise.

4.13 If a complainant does not agree with the University's response, an internal review process is available or a complainant may refer the matter for independent mediation by the Office of the Information Commissioner.

Contracts involving personal information

4.14 Contractual arrangements entered into by the University may require that third parties have access to or may use personal information owned or held by CQUniversity.

4.15 Any contract which is entered into by the University must include appropriate safeguards for protection of personal information. It is the responsibility of the senior officer who has delegated authority to enter into contracts and commercial arrangements, to ensure that privacy risks are adequately addressed and that CQUniversity's privacy obligations are appropriately incorporated into the formal terms of the contract where necessary. For further information, refer to CQUniversity's Contract Management Procedures and Partnerships Policy and Procedure. Queries concerning appropriate contractual provisions covering CQUniversity's privacy obligations may be directed to the Manager, Corporate Governance.

Privacy breach management

4.16 The head of the relevant unit must report any breaches of this policy to the Manager, Corporate Governance or Director, Governance as soon as practicable after the breach has been identified.

4.17 A breach which involves misuse or inappropriate access to personal information by a staff member may be a breach of the University's Code of Conduct and managed under disciplinary or unsatisfactory performance processes.

4.18 Where the matter involves a data breach, the Coordinator, Records and Privacy/Director, Corporate Governance will liaise with the Chief Information and Digital Officer to assist with responding to and reporting on the complaint. The Notifiable Breaches Amendment (2017) was legislated into the Australian Privacy Act in 2018 requiring Australian organisations to notify the Office of the Australian Information Commissioner within thirty days of a breach. The University's Data Breaches procedure is located on StaffNet and assists with data breach classification and how to respond to a breach occurring.

4.19 Management of a privacy breach will include steps to:

- contain the breach
- evaluate the associated risks
- consider notifying the affected individuals, and
- prevention of any further privacy breach.

Review requests

4.20 If an individual believes that their personal information has not been dealt with in accordance with the *Information Privacy Act 2009*, they may make a complaint to the University seeking an internal review. A request for an internal review must be made in writing and must be made within six months from the date when the breach was suspected to have occurred. Requests can be emailed to privacyrti@cqu.edu.au or posted to:

Director, Governance
Governance Directorate
CQUniversity Australia
ROCKHAMPTON QLD 4701

4.21 Requests for review will be acknowledged in writing within 10 business days from the date on which the application was received, and the University will process the request and provide the University's decision in writing within 45 business days from the date on which the application was received.

4.22 If the Director, Governance has previously been involved in the matter to be reviewed, the Vice-Chancellor and President will appoint another senior officer to conduct the review.

4.23 If the applicant does not consider University's review response to be an adequate response, they may lodge a complaint with the Information Commissioner.

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 CQUniversity's obligations under the Act.

5.2 The Director, Governance has general responsibility for privacy management across the University.

5.3 The Director, Governance administers the *Information Privacy Act*, including the following specific responsibilities:

- training staff in the University's privacy obligations
- providing advice on privacy issues
- assisting with the development of privacy notices, and
- coordinating the University's investigation and response to privacy complaints.

5.4 Heads of units are responsible for assessing privacy risk in their area of their responsibility and for implementing business processes consistent with 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 staff within the unit and that 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 unit, and
- ensuring that privacy training and awareness is embedded in practices and procedures of the unit as appropriate.

5.5 Data custodians and record keepers, at both the corporate and local level, are responsible for:

- implementing adequate security measures to protect privacy of personal data in information systems
- determining user access levels for the dataset or system, although the decision to grant access to individual staff may be delegated, and
- implementing appropriate mechanisms to revoke access to systems when access is no longer necessary or appropriate, e.g. when position or formal responsibilities changes, or termination of employment.

5.6 All staff have the responsibility to respect personal privacy as they collect, access, use or disclose personal information about others in the course of their duties, and to comply with the requirements of the *Information Privacy Act* and the specific requirements of this policy and procedure.

5.7 All staff are responsible for ensuring they and their direct reports comply with the requirements of this policy and procedure and the *Information Privacy Act*.

5.8 The Director, Governance has overall responsibility in the implementation and compliance of this policy and procedure. Compliance is monitored through scheduled audits and exception reporting.

Reporting

5.9 Annual reports on access applications processed under the *Right to Information Act* and the *Information Privacy Act* are provided to the Department of Justice and Attorney-General. The Manager, Corporate Governance is responsible for compiling and providing these reports.

Records management

5.10 Staff must maintain all records relevant to administering this policy and procedure in a recognised University recordkeeping system.

6 DEFINITIONS

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

Terms and definitions

Personal information: 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 (section 12, *Information Privacy Act*).

Personal information includes usernames, passwords and unique identifiers such as staff and student numbers. It can be recorded in any format including hard copy documents, electronic documents, databases, administrative systems, photographs and other images, and staff/student identity cards.

Information that is recorded in a way that cannot be linked to a known individual and the personal information has become de-identified, then the Information Privacy Principles do not apply.

7 RELATED LEGISLATION AND DOCUMENTS

Information Privacy Act 2009 (QLD)

Privacy Law, Office of the Australian Information Commissioner

Protecting your right to information and Privacy, Office of the Information Commissioner Queensland

Responding to Police Presence and Police Enquires Procedure

Right to Information Act 2009 (QLD)

Right to Information and Information Privacy Access Application

Website Privacy Statement

8 FEEDBACK

8.1 University staff and students may provide feedback about this document by emailing policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Advisory Committee to Approval Authority	Vice-Chancellor's Advisory Committee
Administrator	Director, Governance
Next Review Date	11/10/2020

Approval and Amendment History	Details
Original Approval Authority and Date	Vice-Chancellor and President 26/06/2014
Amendment Authority and Date	Vice-Chancellor and President 11/10/2017; Administrator Amendment – Director, Governance 14/12/2017, Minor Amendment Approval - Director, Governance 19/08/2019.
Notes	Formerly known as the Privacy and Security Statement.

10 APPENDICES

Appendix 1: Personal information held by CQUniversity

Most personal information held by the University relates to its students and staff. The University may hold other personal information for various purposes of providing services to the University and broader community (such as library membership, gym membership, and alumni contacts). Records may be kept in various offices throughout the University and in a combination of paper-based and electronic formats. Security arrangements will apply, depending on the storage type and sensitivity of the information. Details of specific record handling practices may be obtained from the supervisors of the particular areas.

Student personal information

The University collects personal information for the purposes of providing individuals with information about educational services, for assessment of applications to attend the University, and for enrolling students in courses and programs.

Most student personal information is held on MyCentre, the student enrolment system, and is entered by and capable of amendment by the students personally. Student personal information is also held in other administrative systems. Information may be taken from these systems to populate other University databases including the University's library and IT network systems. Minor collections of personal information on students may be held in other places, such as the Student Residences and the University's customer relationship management system.

University staff who have a need to access student record information (such as student advisors and teaching staff) are entitled to access the student records systems for the purposes of providing services to students. Personal student information is not released to persons outside the University unless the consent of the student has been obtained (for example, for the Queensland Tertiary Admissions Centre), or unless it is required by law (such as by the Australian Tax Office, Department of Immigration and Citizenship, and Department of Industry, Innovation, Science, Research and Tertiary Education).

Student information may be passed to the CQUniversity Student Association as a related but independent body of the University for the purpose of allowing the Association to provide enrolled students with services.

The record of a student's study is held in perpetuity enabling a student to obtain a copy of their academic history from CQUniversity at any time.

Staff personal information

Staff personal information is collected and used for human resource management functions. Such information would include the staff member's application for employment, leave records, and performance management information. This information can be in electronic or paper-based formats. Staff personal information is usually only available to staff who need this information to carry out their duties. Information may be taken from the HR system to populate other University databases including the University's library and IT network systems. Staff records are disposed of in accordance with the approved Retention and Disposal Schedule.

Personal information will only be provided internally to the University where deemed necessary and appropriate in an emergency situation (staff contact details in case of an extreme weather event, or next of kin details in case of an accident) and would only be released to the position supervisor or Associate Vice-Chancellor with strict confidentiality rules applying.

Personal information will not be released to persons outside the University unless the consent of the staff member has been obtained (for example, financial institutions for payroll) or unless it is required by law (such as by the Australian Tax Office or WorkCover Queensland).

Routine employment information of staff which does not relate to the personal aspect of a staff member's employment, such as position title, CQUniversity email address, work phone number, or any information which is publicly available on the University website, is not considered as personal information.

Personal information about vendors

Personal information about vendors may be obtained and held to allow normal business processes associated with the acquisition of goods and services to take place. This information is likely to include name, address for payment, and bank account details to allow for electronic payment of accounts. This information is typically restricted to financial services staff involved in purchasing and accounts payable functions. It is retained as required by law or as set out in the relevant retention and disposal schedule. Periodic examination by external auditors may occur.

Information technology systems records

Central information technology administrators may hold information specific to IT system administration such as security identifiers and usage records for staff and students. Records are kept of external websites visited by staff and students. This information may be disclosed to authorised personnel, including staff supervisors, system administrators and the individual concerned. Users are made aware of system usage rules and procedures through University policies including the Acceptable Use of Information and Communications Technology Facilities and Devices Policy and Procedure.

Unique identifiers

Unique identifiers, such as student and staff numbers, payroll numbers, tax file numbers, credit card numbers or bank account details, are used to record a large amount of personal information. To protect the privacy of students and staff, and to ensure personal information is secure from unauthorised use or disclosure, this information will not be published or made generally available in a way which links to an individual (ie student number not being printed on mailing labels which are sent through the post).

Appendix 2: CQUniversity website

Securing electronic information

The University uses a variety of technologies to secure the information we collect on our servers and to secure the transmission of information. However, there is always a small possibility that an individual's information could be inadvertently disclosed. By using our sites, individuals agree that the University is not liable for the inadvertent or unintentional disclosure of their information.

Some software components of our sites may write small files to individual's computers, known as cookies. These cookies are used to improve the individual's experience and do not contain personally identifying information.

General use

In the normal course of operation of our web servers, CQUniversity collects information about users that may include:

- IP address
- type of operating system and browser
- operating characteristics, like screening resolution and colouring depth
- the URL that referred a user to the site, and
- the part of the world from which the user is accessing the site.

This information is retained and used by web support teams and system administrators to review and improve user experience on the University's site and to diagnose problems. The University does not use this information to identify individual users.

Individuals may supply the University with personal information whilst making electronic requests via the CQUniversity website. This could include requests such as:

- contacting the University or submitting questions – the University may request additional information to be able to assist. This information may include their name, address, email address or other identifying information.
- conducting business with the University electronically - the University may collect additional financial information, including credit card number, expiration date, banking details or billing address.
- performing other functions (ie applications for admission) – the University may collect additional information, including employment and education history, date of birth, phone number or residence status.

If the individual is concerned about transmitting information over the internet, they may choose to contact the University via mail or phone. In this case, the University will not use this information to add the individual to mailings lists or sell this information to commercial third parties.

Authorised use

If an individual accesses the University sites using a password or computer/network connection supplied by the University, the University will retrieve additional information about that user including their identity and relationship the University. This information may be used to assess compliance with relevant University policies on the use of technology and University facilities.

Payments to the University

Personal and financial details requested when paying an account or purchasing something through the University's website are protected at all stages of the transaction.
Credit card details may be encrypted and stored locally while the connection to the credit clearing house is made. Once the transaction is complete, the encrypted details are removed.
Student credit card details, used when paying enrolment fees, are kept in an encrypted form in the student administration system.

Appendix 3: Photographs or recordings taken by CQUniversity

As most images used by CQUniversity are for marketing, communication or media liaison purposes which are available to a national and international community, the University must ensure use of images of individuals is consistent with our privacy obligations.

Types of photography affected

All photographic (still) images and audio/video recordings of staff, students, visitors or members of the public which are used for marketing, publicity and/or corporate communications. Images of professional models, actors or others who are paid a fee for appearing in promotional material or advertisements should be under a commercial or contractual arrangement and are not affected.

Consent

Staff members taking photographs or recordings must obtain consent if:

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

A Talent Release Form must be completed prior to use of any photographic image or recording. The form may be completed after the photograph or recording has been taken, but the image must not be used for University purposes if the individual declines consent.

Talent Release Forms must be kept by the organisational area in accordance with the Retention and Disposal Schedule.

Talent Release Forms are not intended for images or recordings for teaching or research purposes.

Images of children

Parental consent must always be obtained before images of school age or younger children are used in any CQUniversity publication or resource.

Large functions

Where it is impracticable to obtain consent from individuals at large functions or events (such as graduation ceremonies), consent is implied. However, if an individual indicates, either at the function or at a later time, that they do not give their consent, the image cannot be used for CQUniversity publication or communication.

Copyright

Recordings relating to a performance may have copyright implications. If a recording has been produced purely for marketing or communication purposes a consent form can be completed. However, staff members should liaise with the University's Copyright Office to ensure all recordings constituting performances are consented to.

Teaching and research

Teaching – where images or recordings of students are taken for teaching purposes (eg videoing of discussion groups or practical work for later class teaching), a privacy notice should be placed in the unit profile or at the commencement of the class/session.

Research – any recordings required for research should be addressed during the ethical clearance process for the research project in question.

Appendix 4: Requests from law enforcement agencies

If a staff member receives a request from officers of a law enforcement agency the following process for liaison with the external agency must be used.

Requests from law enforcement agencies

If an officer of a law enforcement agency or investigating officer contacts a staff member via the below methods to make an enquiry, seek records or information, or request assistance with an investigation the staff member must:

- Direct the officer to the Associate Vice-Chancellor of the campus and notify the Director, Governance
- In writing or telephone – direct the officer to the Director, Governance
- Outside business hours – refer to the University's Security Office
- Urgent requests – the staff member can provide immediate assistance when the officer is responding to an urgent call regarding the commission of a crime or in response to a report of an emergency situation where there is danger of injury to a person.

Staff member responsibilities

The staff member responsible for managing the request from an officer must:

- establish the bona fides of the officer making the enquiry
- confirm that the disclosure of person information is necessary for law enforcement purposes (ie consider whether there are other means for the officer to obtain the information, for instance relying on legal compulsion, such as use of subpoenas or warrants)
- ensure that only requests for limited named individuals are disclosed and that disclosure of large numbers of groupings of personal records only occur with express legislative authority
- extract information from relevant University records or information systems
- keep a record of the enquiry, and
- notify the Director, Governance of the enquiry and the information provided.

Records

Information Privacy Principle 11 specifies that where personal information has been used or disclosed for law enforcement or revenue protection purposes, the University must "include in the record containing that information a note of the disclosure".

The responsible staff member for managing the request must ensure a log of the enquiry is recorded including the following information:

- the enquiry details including:
  - the date of the enquiry
  - name of organisation requesting the personal information
  - name and contact details of person requesting the personal information
  - nature of information requested
  - source of the personal information requested, and
  - purpose or and justification for disclosure

- what type of personal information was used and/or disclosed, and
- any records such as faxes, emails or file notes generated whilst dealing with the enquiry.

All records, including the log of the enquiry, must be forwarded to the Records Team in the Governance Directorate. This information may be made available for audits or right to information applications, but will not be made available to staff who routinely access the records for normal administrative purposes only.

Appendix 5: Requests from revenue protection agencies

If a staff member receives a request from officers of a revenue protection agency the following process for liaison with the external agency must be used. General advice on the operation of this process may be obtained from Director, Governance.

Requests from revenue protection agencies

Agencies making enquiries may include the Australian Taxation Office, Office of State Revenue or other government agencies that provide benefits or allowances. This process does not apply to standard reporting arrangements by areas under express legislative authority (ie Payroll or Student Governance Centre).

If an officer of a revenue protection agency contacts a staff member to make an enquiry, seek records or information, or request assistance with an investigation the staff member must direct the query to:
- Director, Governance – for student personal information queries
- Director, People and Culture – for staff personal information queries, or
- University Secretary – for all other queries.

Staff member responsibilities

The staff member responsible for managing the request from an officer must:
- establish the bona fides of the officer making the enquiry
- confirm that the disclosure of person information is necessary for the protection of public revenue (ie consider whether there are other means for the officer to obtain the information, for instance relying on legal compulsion, such as use of subpoenas or warrants)
- ensure that only requests for limited named individuals are disclosed and that disclosure of large numbers of groupings of personal records only occur with express legislative authority (the Privacy Guidelines issued by the Commonwealth Privacy Commissioner indicate that it is inappropriate to rely on the law enforcement/revenue protection exceptions to justify disclosure of large amounts of personal data for data-matching purposes)
- extract information from relevant University records or information systems
- keep a record of the enquiry, and
- notify the Director, Governance of the enquiry and the information provided.

Records

Information Privacy Principle 11 specifies that where personal information has been used or disclosed for law enforcement or revenue protection purposes, the University must “include in the record containing that information a note of the disclosure”.

The responsible staff member for managing the request must ensure a log of the enquiry is recorded including the following information:
- the enquiry details including:
  - the date of the enquiry
  - name of organisation requesting the personal information
  - name and contact details of person requesting the personal information
  - nature of information requested
  - source of the personal information requested, and
  - purpose or and justification for disclosure
- what type of personal information was used and/or disclosed, and
- any records such as faxes, emails or file notes generated whilst dealing with the enquiry.

All records, including the log of the enquiry, must be forwarded to the Records Team in the Governance Directorate. This information may be made available for audits or right to information applications, but will not be made available to staff who routinely access the records for normal administrative purposes only.

Appendix 6: Requests from the courts

Under Information Privacy Principle 11, the University may disclose personal information if the University is satisfied on reasonable grounds that the information is necessary for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court of tribunal.

Types of court documents

Court documents includes notices of non-party disclosures, subpoenas or similar court documents where the University is not a party to the court proceedings. A court document will be signed and sealed by a court registrar and issued under the rules of the court.

Requests via court documents

Any requests to release personal information under a court document must be promptly referred to the Director, Governance for action. There can be serious consequences for failure to comply with the requirements of court documents.

Where CQUniversity is named as a party to the proceedings (for example as a defendant or respondent) contact the Director, Governance and University Secretary immediately.

Appendix 7: Requests for a deceased person details

CQUniversity provides the same respect and level of protection for privacy of person information of deceased staff members or students as it is required to provide during life under the *Information Privacy Act*.

Requests

All requests to access personal information of deceased staff members or students must be referred to the Director, Governance who will determine whether the request should be managed under the *Right to Information Act*.