

Information Privacy Policy

Section 1 - Purpose

(1) QUT's functions require the collection, storage, use and disclosure of personal information about students, staff, alumni, donors, partners and other clients. QUT is committed to protecting personal privacy and recognises that individuals have a reasonable expectation that the university will protect and appropriately manage the personal information it holds about them.

(2) QUT must comply with the requirements of the [Information Privacy Act 2009](#) (Qld) which provides for the fair collection and handling of personal information by Queensland public agencies. QUT may be required to comply with other privacy regulations in other jurisdictions to the extent that they apply to its activities, including circumstances where:

- a. QUT has agreed to be contractually bound to manage personal information according to another privacy law, for example the Australian Privacy Principles (APPs) when under contract to the Australian Government or another APP entity, or
- b. a privacy or other law applies to the type of personal information involved, for example tax file number information; or
- c. QUT processes the personal data of an individual who is located in a particular jurisdiction and the law of that jurisdiction applies to the individual's information, for example the European Union General Data Protection Regulation (GDPR).

Section 2 - Application

(3) This Policy applies to the collection, use, disclosure, storage, transfer, handling, right of access, and amendment of personal information at QUT.

(4) It does not apply to:

- a. routine personal work information of staff;
- b. personal information which is maintained on a public register;
- c. information recorded in a de-identified way which cannot be linked (or re-linked) to a known individual;
- d. personal information which is already available in a publication or; and
- e. other publicly available document; or information which is generally available.

Section 3 - Roles and Responsibilities

Position	Responsibility
Vice-Chancellor and President	As the 'principal officer' under the Information Privacy Act 2009 , is responsible for QUT's obligations under the Act.

Position	Responsibility
Vice-President (Administration) and University Registrar	As chief administrative officer, oversees implementation of privacy management across the university, and approves privacy protocols, guidelines and mandatory training arrangements.
Governance Manager (Governance and Performance)	Acts as QUT Privacy Officer, and administers the Information Privacy Act 2009 on behalf of the Vice-President (Administration) and University Registrar, including: 1. making initial decisions on access and amendment applications under the IP Act; 2. training staff in the university's privacy obligations; 3. providing advice on privacy issues; and 4. coordination of the university's investigation and response to privacy complaints and breaches.
Heads of Organisational Units	Manage privacy risk in the organisational unit and implement business processes consistent with the Information Privacy Act 2009 .
Data custodians	Implement adequate security measures to protect privacy of personal information in information systems. Determine user access levels which must be consistent with privacy requirements. Implement appropriate mechanisms to revoke access to systems containing personal information, when access is no longer appropriate, for instance, in the case of a change in position or formal responsibilities, or termination of employment. (The Corporate Information Asset Management Policy provides further details.)
All staff	Undertake required privacy training. Comply with the requirements of the Information Privacy Act 2009 , this Policy and all procedures and Privacy Protocols issued under the policy.

Section 4 - Collection and Use of Personal Information

Collection

(5) Personal information must be collected only where necessary and relevant to QUT'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.

(6) Privacy collection notices must include the following information:

- a. the purposes for collecting the information;
- b. any law or court order that authorises the collection, the title of the law or details of the court order; and
- c. to whom QUT normally discloses the information and, if known, anyone they in turn will disclose it to.

(7) Where a privacy law other than the [Information Privacy Act 2009](#) applies to the personal information collected, a privacy notice may need to include some or all of the following information:

- a. the lawful basis for processing personal information and, if applicable, the legitimate interests for the processing (GDPR);
- b. the retention period for the personal information;
- c. the main consequences for the individual if all or some of the information is not collected;
- d. details of any transfer or storage of the information outside Australia and how privacy is protected in such circumstances;
- e. how individuals can request access to, or amendment of their personal information, or exercise their legal rights;

- f. the contact details of the University or the head of the organisational area, the QUT Privacy Officer and a link to this Information Privacy Policy;
- g. where personal information is collected from a third party, the source and the categories of personal information collected;
- h. the details of any automated decision-making or profiling where relevant.

Use

(8) 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.

(9) Further guidance on use of personal information is detailed in the [Privacy Protocols](#) (QUT staff access only).

Section 5 - Access and Security of Personal Information

(10) 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 Policy](#) provides further details on how to classify and protect personal information.

Section 6 - Prohibition on Disclosure of Personal Information

(11) 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 QUT will cease to have effective control of the information once it is released.

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

- a. where there is appropriate documentary evidence that the individual has agreed to disclosure;
- b. where a privacy notice given at the point of collection advises the individual about the usual practices for disclosure;
- c. where disclosure is required or authorised by law (for example, court order or subpoena, legislative obligation to disclose);
- d. 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
- e. where disclosure is necessary for investigation or enforcement of criminal matters or other law enforcement matters.

(13) [Privacy Protocols](#) (QUT staff access only) which set out the considerations and procedures for disclosure of personal information in these circumstances are available and must be followed. Disclosing personal information in other situations must only occur following confirmation from the Privacy Officer that disclosure is necessary and acceptable under other limited provisions in the [Information Privacy Act 2009](#).

Section 7 - Register of Graduates

(14) QUT, 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, through the [Verification of Qualifications](#) service. The only details confirmed through this service are the graduate's name (as recorded in QUT systems), the degree conferred or to be conferred and the date of conferral. QUT may charge a fee for this service.

Section 8 - Requests for Access to and Amendment of Personal Information under Information Privacy Act 2009

(15) The [Information Privacy Act 2009](#) also provides a right of access to, and amendment of, personal [information](#). Details on how an individual can request access to or to amend their personal information in accordance with the [Information Privacy Act 2009](#) can be found in the university's [Information Access Policy](#) webpage [Requesting Access to and Amendment of your Personal Information under Information Privacy](#).

Section 9 - Privacy Complaints

(16) If an individual believes that QUT has not dealt with their personal information in accordance with the [Information Privacy Act 2009](#) or this Policy, they may make a [Privacy Complaint](#) to QUT. A complaint must be made in writing or by email to the Privacy Officer or referred to that officer if received by another area of the university.

(17) Primary responsibility for investigating and responding to the complaint will rest with the head of the organisational unit concerned, with advice from the Privacy Officer 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.

(18) 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.

Section 10 - Privacy Breach Management

(19) The head of the relevant organisational unit must report any breaches of this Policy to the Privacy Officer as soon as practicable after the breach has been identified. Where the matter involves a breach of information security, the Privacy Officer will liaise with the Manager, [Information Security](#) to assist with responding to and reporting on the complaint.

(20) Management of a privacy breach will include steps to:

- a. contain the breach;
- b. evaluate the associated risks;
- c. consider notifying the affected individuals; and
- d. prevention of any further privacy breach.

(21) The Vice-President (Administration) and University Registrar must be informed of serious breaches of this Policy or related protocols and any actions arising out of any investigations.

(22) A breach which involves misuse or inappropriate access to personal information by a staff member may be a breach of the [Code of Conduct - Staff](#) and managed under disciplinary or unsatisfactory performance processes.

Section 11 - Implementation of Privacy Obligations

(23) Protection of personal information must be addressed as part of many university activities. These activities include:

- a. ensuring commercial contracts with third parties have appropriate safeguards for protection of personal information, consistent with QUT's policy on [Contracts and Legal Instruments Management Policy](#);
- b. addressing requirements of the Information Privacy Act (IP Act) when transferring personal information outside of Australia; and
- c. ensuring that unique identifiers are not published or made generally available.

Section 12 - Privacy Impact Assessment

(24) [Privacy Impact Assessments](#) (PIA) (QUT staff access only) assist Project Managers, data custodians and heads of organisational areas to appropriately consider and manage privacy. A PIA should be undertaken throughout the development and implementation of a project or new business process that collects, uses, or discloses personal information, or when making significant changes to existing systems or processes.

Section 13 - Definitions

Term	Definition
Australian Privacy Principles	Means the set of 13 principles in the Privacy Act 1988 (Cth) governing the collection, quality, use, disclosure, management and transfer of personal information.
General Data Protection Regulation (GDPR)	Means the legal framework governing the collection and processing of personal information of individuals located in the European Union (EU).
Information Privacy Principles	Means the set of 11 principles in the Information Privacy Act 2009 governing the collection, use, disclosure, management and transfer of personal information by organisations such as the university.
Personal Data	Has the meaning given to it in Article 4 of the GDPR.
Personal Information	Is as defined by the Information Privacy Policy 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. 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.
A Privacy Breach	A privacy breach occurs when there is a failure to comply with the information privacy policy or the Information Privacy Act 2009 11 privacy principles. Usually this will result in unauthorised disclosure of or unauthorised access to personal information.
A Privacy Complaint	Is a complaint about an act or practice of QUT in relation to an individual's personal information that is a breach of this Policy or the Information Privacy Act 2009 .
Unique Identifiers	Unique identifiers including student and staff numbers are used as the basis for recording a large amount of personal information. Other unique identifiers include payroll numbers, tax file numbers, credit card numbers and bank account details.

Term	Definition
Routine Employment Information	Routine employment information of staff is any information which does not relate to the personal aspects of a staff member's employment at the university. This includes information such as a staff member's position title, QUT email address, work phone number or any information which is publicly available on the QUT website.

Section 14 - Delegations

(25) Refer to [Register of Authorities and Delegations](#) (VC004, VC005) (QUT staff access only).

Status and Details

Status	Current
Effective Date	14th October 2022
Review Date	1st October 2027
Approval Authority	Vice-Chancellor and President
Approval Date	14th October 2022
Expiry Date	Not Applicable
Policy Owner	Sonya Betros Director, Governance and Performance
Author	Sonya Betros Project Manager
Enquiries Contact	Sonya Betros Director, Governance and Performance