Privacy Management - Procedures

1. Purpose

1.1 These procedures provide a structured approach to the University's management of personal information.

Privacy management considers how personal information is treated while it is within the University's responsibility.

1.2 The concepts and principles from the Privacy and Right to Information - Operational Policy are operationalised through these procedures, with obligations under legislation also contextualised for University functions.

1.3 These procedures must be read in conjunction with the linked Privacy and Right to Information - Operational Policy, Data Governance – Operational Policy, Right to Information - Procedures, Data Breach - Procedures, Data Handling – Guidelines (login required) and Personal Data Collection – Guidelines (login required).

2. Scope and application

2.1 These procedures apply to all University staff, students undertaking research or involved in other University business, approved third parties, alumni, contractors, and sub-contractors. It includes all individuals who handle University data and information, regardless of their role or affiliation.

2.2 These procedures apply to all University data and information.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

3 December 2024

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2026

STATUS

Active

4. Protection of privacy and access to information

4.1. The University is committed to protecting the personal information of individuals it engages with throughout every aspect of its business, and at every stage of the data lifecycle, in accordance with the Privacy and Right to Information - Operational Policy, Data Governance – Operational Policy, and requirements under legislation.

4.2 The rights of individuals to access and amend their personal information are respected. Proactive amendment of personal information is encouraged to ensure it remains complete, up to date, accurate and reliable to support University functions.

4.3 The University supports individuals when additional rights apply, including when legal powers can be applied beyond international territorial boundaries. This includes consideration of the scope of obligations imposed under applicable state, national and international legislation, such as the General Data Protection Regulation, which applies for residents of the European Economic Area, and the Data Protection Act 2018 in the United Kingdom.

4.4 The University takes a "privacy by design" approach to embed privacy management practices and protection of personal information into business systems, processes, and functions. Underpinning this strategy is the use of privacy assessments (login required) to proactively identify privacy considerations for new or changed approaches to handling personal information.

4.5 Individuals can make a complaint to the University when they believe it has not met its obligations under the *Information Privacy Act 2009 (Qld)*. Further information about this process is available on the University's Privacy webpage.

5. Management of personal information throughout the data lifecycle

5.1 Responsible management of personal information applies throughout all stages of the University's data lifecycle, depicted in Figure 1: Data lifecycle, and in accordance with Data Governance – Operational Policy and Data Management - Procedures. Practical guidance for University staff is available on MyUniSC (login required).

Figure 1: Data lifecycle

5.2 Capture

5.2.1 Personal information is obtained directly from individuals where practicable, or from authorised third parties and in accordance with the Personal Data Collection – Guidelines (login required).

5.2.2 Collection of personal information is minimised to only what is required to carry out University functions and activities and collected in a fair and lawful way.

5.2.3 When personal information is collected directly from individuals, the University informs them of:

(a) what personal information is being collected and held;

(b) the purpose for collection, use and disclosure of personal information;

(c) the relevant law or order requiring or authorising collection (where applicable);

(d) how an individual can access or amend their personal information;

(e) any potential impacts of not providing personal information;

(f) third parties the University can disclose the personal information to; and

(g) whether the personal information is to be transferred outside of Australia.

5.2.4 When consent is obtained from individuals for the collection and use of personal information, the following conditions must be met:

(a) consent must be provided voluntarily by individuals;

(b) individuals must be sufficiently informed of the proposed use or disclosure of their personal information;

(c) consent requested must be specific for a proposed use and/or disclosure of personal information; and

(d) individuals must be provided with the opportunity to review, withdraw, or renew their consent preferences to ensure currency of consent.

5.2.5 Individuals can withdraw their consent given in connection with any processing of their personal information. This does not impact any processing undertaken prior to such withdrawal.

5.2.6 Unless required by law, consent must be obtained to use data for any purpose not originally disclosed to individuals (additional purpose), or for the collection of sensitive information or personal information from children.

5.3 Store

5.3.1 Personal information in digital form must be stored in an appropriate University approved business system (login required) to support the relevant business functions.

5.3.2 Physical copies of personal information must be stored in an appropriately secured University location.

5.3.3 When under the University's control, personal information must be protected from:

(a) loss, interference or damage;

(b) unauthorised access or disclosure;

(c) modification or use that is not permitted; and

(d) any other form of misuse.

5.3.4 Technical and access controls must be applied in alignment with the classification of personal information, as defined in the Data Classification - Procedures, and in alignment with the ICT Security - Operational Policy and associated procedures.

5.3.5 Handling of personal information must be in accordance with the Data Handling – Guidelines (login required), and the Closed Circuit Television (CCTV) and Security Recordings - Operational Policy. The University's approach to data breach management is outlined in the Data Breach - Procedures.

5.4 Utilise

5.4.1 The University must only use personal information for the purpose individuals were informed of, or for a permitted additional and unrelated purpose as defined under legislation. This includes using personal information:

(a) when the individual has provided their consent for the additional and unrelated use;

(b) as required to mitigate serious risk to an individual or the public, including risks to life, health, safety and wellbeing;

(c) as necessary for law enforcement activities and emergencies; or

(d) when it is otherwise authorised or required by law.

5.4.2 Data Custodians are responsible for providing guidance on appropriate use of personal information and must approve the use of personal information for a permitted additional and unrelated use.

5.4.3 When the use of personal information does not require it to be identifiable, the de-identification, anonymisation, or aggregation of data is encouraged to protect the privacy of individuals.

5.5 Share

5.5.1 Sharing or disclosing personal information with third parties outside the University must be limited to situations the individual is informed of or has consented to, or as otherwise permitted under legislation.

5.5.2 Other permitted uses include to mitigate serious risk to an individual or the public, for law enforcement purposes, or if otherwise required or authorised under legislation.

5.5.3 When personal information is shared with a third party for the purpose of data processing, including contractors or sub-contractors, the University must take reasonable steps to ensure the third party adheres to the requirements of the Privacy and Right to Information - Operational Policy, these procedures, the *Information Privacy Act 2009 (Qld)*, and any other applicable compliance obligations.

5.5.4 In certain circumstances, it can be necessary to transfer personal information across jurisdictional borders.

5.5.5 When personal information is transferred outside of Australia, or transferred into Australia from individuals residing overseas, individuals must be notified of the cross-border data transfer, in compliance with the applicable legislation.

5.5.6 When personal information is transferred outside of Australia, the transfer must be compliant with the University's obligations under Section 33 of the *Information Privacy Act 2009 (Qld)*.

5.6 Archive

5.6.1 Records containing personal information must be archived securely, comply with the University's obligations under the *Public Records Act 2023 (Qld)* and be in accordance with the Records Management – Procedures.

5.7 Dispose

5.7.1 Personal information is securely disposed of when no longer required by the University to meet a business need, legal requirement, or compliance obligation.

5.7.2 Disposal of University records containing personal information must be completed in accordance the Records Management – Procedures.

6. Monitoring and reporting

6.1 Regular monitoring and reporting on the application of privacy management procedures are reported to the Data Analytics and Information Management Advisory Committee.

6.2 The Chief Data Officer monitors and reports on University compliance with these procedures in accordance with the Compliance Management Framework - Governing Policy.

6.3 The University reports each financial year in relation to its compliance with its reporting obligations under Section 6 of the *Information Privacy Regulation 2009 (Qld)* and Section 8 of the *Right to Information Regulation 2009 (Qld)*.

7. Authorities and responsibilities

7.1 As the Approval Authority the Chief Operating Officer approves these procedures to operationalise the Privacy and Right to Information - Operational Policy.

7.2 As the Responsible Executive Member the Chief Operating Officer can approve guidelines to further support the operationalisation of these procedures. All procedures and guidelines must be compatible with the provisions of the policy they operationalise.

7.3 As the Designated Officer the Chief Data Officer is authorised to approve associated documents to support the application of these procedures.

7.4 These procedures operate from the last amended date, and all previous iterations of policy documents related to privacy management are replaced and have no further operation from this date.

7.5 All records relating to privacy management must be stored and managed in accordance with the Records Management – Procedures.

7.6 These procedures must be maintained in accordance with the Policy Framework - Procedures and reviewed on the shortened 2-year policy review cycle.

7.7 Any exception to this policy to enable a more appropriate result must be approved in accordance with the Policy Framework - Procedures prior to any deviation from these procedures.

7.8 Refer to Schedule C of the Delegations Manualin relation to the approved delegations detailed within this policy document.

7.9 Privacy Management Roles

7.9.1 The following roles, responsibilities and accountabilities are specific to these procedures and cascade from the high-level roles and responsibilities in the Privacy and Right to Information - Operational Policy and the Data Governance – Operational Policy.

ROLE	POSITION	AUTHORITY, RESPONSIBILITIES, ACCOUNTABILITIES
Data Champion	Vice-Chancellor and President	Identified as the Principal Officer under the *Information Privacy Act 2009 (Qld)*. Accountable for: (a) appointing powers under the *Information Privacy Act 2009 (Qld)* to an approved delegate.
Chief Data Officer	Chief Data Officer	Appointed as the approved delegate for the *Information Privacy Act 2009 (Qld)*. Accountable for: (a) ensuring compliance with the University's obligations under the *Information Privacy Act 2009 (Qld)*; and (b) assurance for privacy-related risks. Responsible for: (a) embedding procedural and legislative requirements for privacy management; (b) appointing data custodians and ensuring they are inducted; (c) implementing procedures and supporting guidance to embed responsible and compliant privacy management practices; and (d) regular reporting to data and information committees on privacy compliance and practices.
Data Custodian	Heads of Business areas (Appointed by the CDO)	Responsible for: (within their data domain) (a) identifying appropriate approved University business systems for storage of personal information within their data domain; (b) providing guidance on acceptable uses of personal information in alignment with the purpose it was collected for, and approving any permitted additional and unrelated use of personal information as defined under legislation; and (c) identification of privacy related risks and implementation of mitigation strategies to control.
Business System Owners	In accordance with the ICT Security – Operational Policy	Responsible for: (a) implementing technical controls within their business systems to ensure the protection of personal information.

Data Subject Matter Experts	Staff based on specific expertise-criteria relative to a data asset.	Responsible for: (a) providing expertise for business considerations relating to privacy management.
Data Users	All University staff or affiliates that create and use University data and information.	Responsible for: (a) understanding their rights and responsibilities under these procedures; (b) handling personal information in a responsible and compliant manner; (c) applying the appropriate data classification to personal information they are capturing or handling; and (d) adhering to the requirements in these procedures.

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Operational Policy
- Closed Circuit Television (CCTV) and Security Recordings - Operational Policy
- Compliance Management Framework - Governing Policy
- Compliance Management Framework - Procedures
- Data Breach - Procedures
- Data Classification - Procedures
- Data Management - Procedures
- ICT Security - Operational Policy
- Records Management - Procedures
- Risk Management - Governing Policy
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Data Breach - Procedures
- Data Governance - Operational Policy
- Privacy and Right to Information - Operational Policy
- Right to Information - Procedures

RELATED LEGISLATION / STANDARDS

- Public Records Act 2023 (Qld)
- Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)
- Information Privacy Act 2009 (Qld)
- Invasion of Privacy Act 1971 (Qld)