Privacy and Right to Information - Operational Policy

1. Purpose

1.1 This policy outlines the University's approach for information privacy ensuring responsible handling and protection of personal information of individuals who interact with the University, and its proactive provision of access to information for the community, in compliance with the University's legislative obligations.

1.2 As a public authority established under the *University of the Sunshine Coast Act 1998 (Qld)*, the University is committed to publishing or providing access to information it holds, unless doing so would be contrary to the public interest, or a breach of privacy or confidentiality.

1.3 This policy must be read in conjunction with the linked Privacy Management - Procedures, Right to Information - Procedures and Data Governance - Operational Policy.

2. Scope and application

2.1 This policy applies 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 This policy applies 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

Vice-Chancellor and President

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 2029

STATUS

Active

4. Policy statement

4.1 The University promotes the protection of personal information, including sensitive information, in every aspect of its business and fosters a culture of information privacy protection and responsible access. It respects the trust placed in it by the community to collect and handle personal information responsibly and in compliance with legislation and will act transparently when collecting and handling personal information, enabling individuals to understand and exercise their rights. It recognises the protection of privacy is a shared responsibility between individuals and the University.

4.2 The University is committed to publishing or providing access to information it holds, in accordance with its obligations as a public agency. A decision to publish or disclose information balance the considerations of privacy, confidentiality, legislative obligations, and public interest.

4.3 This policy should be read with the University of the Sunshine Coast's website page on Privacy, which outlines the University's personal data processing, information access and privacy complaints practices.

5. Principles

5.1 The University has adopted 5 principles that underpin its approach to data privacy and information access.

5.2 Upholding and respecting the information privacy rights of individuals is fundamental to University operations.

5.2.1 Individuals are informed of personal information use and disclosure at the time of collection. Personal information is collected from individuals in an ethical and lawful manner. All reasonable steps are taken to ensure personal information remains complete, accurate and up to date, and that individuals can amend their personal information. When consent is obtained for the collection, use and disclosure of personal information, individuals are provided with the means to withdraw or update their consent preferences.

5.2.2 The types of information the University is in possession of or controls about an individual is also available to that individual. The University is responsive to privacy complaints and manages these in accordance with the *Information Privacy Act 2009 (Qld)*.

5.3 The University is transparent and open about information for which it is responsible.

5.3.1 The University is committed to acting with transparency and openness regarding the information it manages. It recognises its obligations under the *Right to Information Act 2009 (Qld)* and *Information Privacy Act 2009 (Qld)* to provide pathways for individuals to access information. The University also proactively releases information where appropriate through its Publication Scheme.

5.3.2 Details for requesting access to information the University holds, including personal information, are provided on the Right to Information webpage.

5.4 Protection of personal information is essential across University business.

5.4.1 The protection of personal information is prioritised throughout its lifecycle at the University. Methods for collecting, storing, using, transferring, and disclosing personal information encompass privacy and security considerations, and access is limited to only those who require it to carry out functions or activities of the University.

5.4.2 Personal informationis securely disposed of or de-identified once it is no longer required for business needs or under legislation. In the event of a known or suspected privacy breach, the University proactively implements strategies to minimise potential harm to individuals in accordance with the Data Breach - Procedures.

5.5 Collection and use of personal information is minimised to safeguard an individual's privacy.

5.5.1 Collection of personal information is minimised to only necessary information, that supports functions and activities of the University.

5.5.2 The University only collects, uses, discloses or transfers personal information for a purpose that an individual has been informed of, or as required by law.

5.5.3 When applicable, de-identified information is used to support University business activities where identification of individuals is not necessary.

5.6 'Privacy by design' is embedded across the University.

5.6.1 The University utilises a 'privacy by design' approach, which proactively embeds privacy controls and practices into design and architecture specifications for technology, infrastructure, and business processes. This ensures personal information is safeguarded from misuse, loss, interference, unauthorised access, modification, or disclosure, through a combination of controls applied to people, processes, and technology.

5.6.2 Privacy assessments are undertaken for activities that collect, use, manage or disclose personal information to proactively identify and mitigate risks.

6. Monitoring and reporting

6.1 Regular monitoring and reporting on the application of the privacy and right to information policy and related procedures, is reported by the Chief Data Officer on a quarterly basis to the Data Analytics and Information Management Advisory Committee.

6.2 The Chief Data Officer monitors and reports on the University's compliance with this policy 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 Vice-Chancellor and President approves this policy in accordance with the *University of the Sunshine Coast Act 1998 (Qld)*.

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

7.3 As the Designated Officer the Chief Data Officer can approve associated documents to support the application of this policy. All associated documents must be compatible with the provisions of the policy.

7.4 This policy operates from the last amended date, with all previous iterations of policy related to privacy and right to information replaced and having no further operation from this date.

7.5 All records relating to privacy and right to information must be stored and managed in accordance with the Records Management - Procedures.

7.6 This policy must be maintained in accordance with the Policy Framework – Procedures and reviewed on the standard 5-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 deviation from the policy.

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

7.9 Privacy and Right to Information roles

7.9.1 The assignment of privacy and right to information roles with their associated accountabilities and responsibilities are fundamental for the protection of privacy at the University. Formally appointed roles include that of Data Custodian, in accordance with 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)* and *Right to Information Act 2009 (Qld)*. Accountable for: (a) appointing powers under the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld)* to an approved delegate.
Chief Data Officer	Chief Data Officer	Delegated officer for legislative powers and functions under the *Information Privacy Act 2009 (Qld) and Right to Information Act 2009 (Qld)*. Accountable for: (a) ensuring compliance with the University's obligations under the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld)*; and (b) assurance for privacy-related risks. Responsible for: (a) implementation, oversight, and advocacy for the University's privacy and right to information approach and related initiatives; (b) promoting the University's privacy and right to information policy documents; (c) appointing data custodians and confirming induction of appointed individuals; (d) regular reporting to data and information committees on privacy compliance and practices; (e) providing direction for identification and management of privacy-related risks; and (f) incorporating privacy and right to information responsibilities within relevant University governing committees with appropriate decision-making powers.
Data Custodian	Heads of Departments (appointed by CDO)	Responsible for: (within their data domain) (a) implementing local business processes and appropriate controls for the collection and use of personal information consistent with University policy documents and obligations under the Information Privacy Act 2009 (Qld); (b) ensuring adherence to the University's business processes for right to information requests in accordance with University policy documents, and the Information Privacy Act 2009 (Qld) and Right to Information Act 2009 (Qld); 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; (b) regular interfaces with Data Custodian to align expectations for the protection of privacy in their data domain.
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 obligations for responsible and compliant collection and handling of personal information in accordance with University policy documents and the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld);* and (b) adhering to University business processes for right to information requests in accordance with University policy documents, and the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld)*.

END

RELATED DOCUMENTS

- Compliance Management Framework - Governing Policy

- Compliance Management Framework - Procedures
- Critical Incident Management - Operational Policy
- Data Breach - Procedures
- Data Classification - Procedures
- Data Management - Procedures
- ICT Access Control - Operational Policy
- ICT Security - Operational Policy
- Incident Management - Procedures
- Records Management - Procedures
- Risk Management - Governing Policy
- Risk Management - Procedures
- University Audit and Assurance - Governing Policy
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Data Governance - Operational Policy

- Privacy Management - Procedures
- Right to Information - Procedures

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)
- Information Privacy Act 2009 (Qld)
- Human Rights Act 2019 (Qld)
- Electronic Transactions Act 1999 (Cth)
- Freedom of Information Act 1982 (Cth)