Right to Information - Procedures

1. Purpose

1.1 These procedures provide a structured approach to the University's management of access to information. Right to information considers how personal and other University information is shared with staff, students, and the public.

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 and Administrative Information Release - 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.

4. Managing right to information

4.1 The University is committed to openness and transparency, whilst protecting individuals' privacy, confidentiality, and the public interest. This approach is in alignment 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 their personal information are respected.

4.3 The proactive release of routine information is encouraged, based on data classification in accordance with Data Classification - Procedures, privacy considerations, and Data Custodian oversight. This ensures streamlined release of information where appropriate, thereby reducing time and costs compared to formal Right to Information applications.

4.4 The University supports individuals when additional rights apply, considering the scope of obligations imposed under applicable state, national and international legislation.

4.5 The University has a Publication Scheme that proactively makes available a broad range of information about its operations to the public, through its website and other channels. This includes a Disclosure Log of previously released information considered to be of significant interest to the wider public.

4.6 Responsible release of information applies during the 'Share' stage of the data lifecycle in accordance with Data Governance – Operational Policy. When considering the release of information, the University is responsible for balancing a requestor's rights under legislation with privacy and confidentiality considerations. This includes the consideration of data classification based on its level of sensitivity in accordance with Data Classification - Procedures, the risk it presents and legislation that protects it.

4.7 Data Custodians provide assurance and oversight by governing data access in their respective areas, including the review and endorsement for release of information.

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

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

5. Access to information

5.1 Requests to access information proactively depend on the demand and any possible significant adverse impacts likely to result from disclosure. The University can decide against providing access on the grounds that the information:

(a) is exempt information under the Acts;

(b) would impact on the privacy of other individuals;

(c) is contrary to the public interest to release;

(d) is subject to legal proceedings;

(e) is not in a child's best interest;

(f) is prejudicial to the physical or mental health or wellbeing of the applicant;

(g) does not exist or cannot be located;

(h) other access is available.

5.2 The University only provides the relevant information requested, to prevent additional or an excessive disclosure of information occurring.

5.3 When disclosure of information would reasonably be expected to be of concern to a third party, then the University takes reasonable steps to obtain the views of the relevant third party.

5.4 In the event of an accidental or unlawful disclosure of information, the University would enact the Data Breach - Procedures.

6. Verifying identity and authority

6.1 Before sharing a person's personal information, the University must:

(a) verify the identity of the individual as the requesting person; and

(b) where applicable, verify the identity and authority of the representative acting on behalf of the individual.

6.2 Further information on verification of identity is outlined in the Administrative Information Release - Guidelines (login required).

7. Surveillance technology

7.1 CCTV is used across University campuses in public spaces for the purposes of public safety. Release of CCTV footage must be in accordance with the Closed Circuit Television (CCTV) and Security Recordings - Operational Policy.

8. Personal information disclosure

8.1 Personal information can be disclosed when the University considers it necessary to lessen or prevent serious threat to an individual or the public or is otherwise required. This can include:

(a) disclosure to law enforcement agencies for law enforcement activities;

(b) other relevant third parties in emergency situations; or

(c) when authorised or required by law.

8.2 The University can disclose personal information to a range of Commonwealth, state and territory entities as part of mandatory reporting requirements, authorised under a law or contractual obligation.

8.3 When disclosure is necessary for research in the public interest, the following applies:

(a) the information is de-identified before publication or disclosure;

(b) the express or implied agreement of the individual concerned is not practicable to obtain before the disclosure; and

(c) the University is satisfied on reasonable grounds that the entity the University discloses it to will not disclose the personal information to another entity.

9. Monitoring and reporting

9.1 Regular monitoring and reporting on the application of the Right to Information - Procedures are reported to the Data Analytics and Information Management Advisory Committee.

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

9.3 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)*.

10. Authorities and responsibilities

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

10.2 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.

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

10.4 These procedures operate from the last amended date, and all previous procedures related to right to information are replaced and have no further operation from this date.

10.5 All records relating to right to information must be stored and managed in accordance with the Records Management – Procedures.

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

10.7 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.

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

10.9 Right to Information Roles

10.9.1 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)* 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	Appointed as the approved delegate for 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) embedding procedural and legislative requirements for right to information management; (b) appointing Data Custodians and ensuring they are inducted; (c) implementing procedures and supporting guidance to embed responsible and compliant right to information practices. (d) decision-making for formal right to information requests.

Reviewer	Equivalent or higher to Chief Data Officer	Appointed to internally review reviewable decision made under the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld)* to an approved delegate.
Data Custodian	Heads of Departments (appointed by the CDO)	Responsible for: (within their data domain) (a) identifying appropriate approved University business systems for storage of information within their data domain; (b) approving access and sharing requests for personal information within their data domain; (c) approving administrative release of routine information within their data domain; (d) providing oversight and advice for the release of information under formal Right to Information requests.
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 right to information.
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) sharing information in a responsible and compliant manner; (c) 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
- Privacy Management - Procedures
- Records Management - Procedures
- Risk Management - Governing Policy
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Incident Management - Procedures

- Privacy and Right to Information - Operational Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Information Privacy Act 2009 (Qld)
- Freedom of Information Act 1982 (Cth)