Data Handling Procedure

Section 1 - Purpose and Scope

(1) This Procedure outlines data handling requirements for all data, information and records at The University of Queensland (UQ). Members of the UQ community who handle UQ data and information must comply with this Procedure. This includes (but is not limited to) students, staff, contractors and consultants, visitors, title holders and third parties.

(2) The requirements and controls outlined in this Procedure aim to:

a. protect UQ's community and information;
b. reduce UQ's cyber security risk;
c. enable safe and ethical information use; and
d. ensure compliance with UQ's legislative obligations.

(3) This Procedure should be read in conjunction with the Information Governance and Management Framework, the Information Management Policy, and associated policies and procedures including:

a. Information Security Classification Procedure
b. Records Management Procedure
c. Access to and Amendment of UQ Documents Procedure
d. Privacy Management Policy and Privacy Management Procedure
e. Research Data Management Policy
f. Enterprise Data Ethics Framework
g. Cyber Security Exceptions Procedure
h. supporting IT procedures, frameworks and standards.

Section 2 - Process and key controls

(4) Individuals must:

a. Handle data and information according to their information security classification;
b. Use UQ-approved IT services throughout the information lifecycle. Contact IT support to raise any queries about services;
c. Comply with UQ and IT procurement processes and requirements if acquiring new information systems or services. Visit the ICT Procurement webpage for more information;
d. Limit the collection, use, retention, disclosure or sharing of personal, SENSITIVE or PROTECTED information (e.g. driver's licence details, student grades linked to student identity, health data). Deidentify data wherever possible;
e. Wherever possible, use existing data instead of recapturing or duplicating data. For information on accessing UQ data, visit the Access and Share Data webpage for corporate data, and the Library guide for research data;

f. Comply with any local processes and practices regarding data handling and information systems;
g. Use UQ-managed devices (laptops, desktops and mobile devices if provided) where possible;
h. Seek advice from cyber security, information and records management teams as required (see Appendix for details); and
i. Align with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research when handling Indigenous data, noting that the code's principles apply to research and other activities that can impact upon, or be of importance to, Aboriginal and Torres Strait Islander peoples.

Exceptions

(5) Exceptions to this Procedure (e.g. if certain requirements cannot be met) must be managed in accordance with the Cyber Security Exceptions Procedure.

Additional obligations

(6) Information Domain Custodians are responsible for ensuring that specific industry or research requirements (e.g. Australian Code for the Responsible Conduct of Research, Payment Card Industry Data Security Standard) are identified within their assigned domains, and that appropriate controls are implemented.

(7) Additional or alternative controls may also apply to UQ data and information associated with a contract, licence or agreement (e.g. a data sharing agreement).

Additional research obligations

(8) Staff (including contractors) and HDR candidates must adhere to the research data management classifications and controls that are specified in the relevant contractual agreements or ethics approvals.

(9) They must also define additional or alternate classifications and associated controls in a research data management plan (to be stored in UQRDM) for the following types of information:

a. National security information: additional controls may apply if staff create or capture information that if subject to a data breach, would damage the national interest or have national security implications. Refer to the Australian Government Protective Security Policy Framework.
b. Defence Industry Security Program (DISP): alternate security controls apply if staff capture or create information as part of a DISP research project. Contact Research Ethics and Integrity at international.safeguards@uq.edu.au for more information.

(10) See the Research Data Management Policy for more information on research data management plans.

Section 3 - Key Requirements

(11) The UQ community must manage data and information appropriately throughout the information lifecycle. In each phase of the information lifecycle, controls and requirements apply based on the information security classification and these are defined in the sections below.

(12) Requirements in the 'plan and design' phase apply throughout the lifecycle.

Plan and Design

(13) Individuals must comply with the following requirements (as relevant):

a. Research data: for each research project, a First Named Investigator (also referred to as Lead Chief

Investigator) and the relevant organisational unit must be identified at the start of the project. The First Named Chief Investigator assumes the role of the Information Steward for the duration of the project. Upon project completion (or departure from UQ), the role of Information Steward transfers to the identified Head of School or Director of Institute. See the Administration of Research Funding - Applications, Grants and Contract Research Policy for criteria for the First Named Chief Investigator role.

b. Access policies: Information Domain Custodians are responsible for approving access policies (including any changes) for their information domains. Individuals should only be given access to the data required to execute their responsibilities. Access policies must be reviewed periodically in line with the Access and Privileges Management Framework.
c. Use UQ-approved IT services throughout the information lifecycle. If procuring a new IT service, or using any other non-UQ approved IT service to handle data, comply with the Software Acquisition and Use Procedure, the ICT Procurement Framework and the Procurement Policy. Consult Information Technology Services (ITS) to ensure that all legislative, security and information management requirements are met.
d. Consider any future requirements regarding records retention, disposal, archiving, decommissioning systems, transfer of data, and ongoing management.
e. Consider metadata when identifying data entry/capture requirements.
f. Consider any risks (including cyber security risks) associated with the information or IT services being used. If required, conduct a risk assessment in alignment with the Enterprise Risk Management Framework.

Privacy Impact Assessments (PIAs)

(14) When proposing new or changed IT services or processes that will handle personal information, a PIA may be required.

a. At a minimum, if a proposed new IT service (or changes to an existing service) will handle personal information, staff (e.g. the project team) should undertake a Threshold Privacy Assessment (TPA) to determine whether a PIA is required. TPAs should be submitted to the relevant Information Steward(s) and the Right to Information and Privacy Office (RTI and Privacy Office).
b. Information Stewards are responsible for conducting PIAs, which must be reviewed by the RTI and Privacy Office and approved by the relevant Information Domain Custodian. The approved PIA must be provided to the RTI and Privacy Office for record keeping.

(15) Resources and templates for TPAs and PIAs are available under the Staff Resources section of the RTI and Privacy Office website.

Data sovereignty

(16) The location and jurisdiction of services used to store/process data must be considered to ensure UQ's legislative and security requirements are met.

(17) To avoid risks associated with data sovereignty, only use appropriate UQ-approved IT services throughout the information lifecycle and consult ITS regarding use of any new IT services.

(18) When cloud services are utilised, consideration must be given to the cloud service provider country of origin, regardless of the location in which the data is stored. In certain circumstances, laws in the jurisdiction in which the company is based (or where the data is stored/processed) may mean third parties (including government entities) within that country could access the data. Data sovereignty restrictions also apply to offline data (e.g. backups).

(19) When considering data hosting outside Australia or situations where a vendor can access data from another country (e.g. to provide user support), the following requirements apply:

a. Personal information may only be transferred outside of Australia (including the storage of personal information in cloud-based services on servers located outside of Australia) in compliance with section 33 of the Information Privacy Act 2009 (Qld). Where personal information is proposed to be transferred offshore, a Privacy Impact Assessment should be undertaken to ensure all compliance obligations are met - see clauses 14-15 above for more details.
b. SENSITIVE and PROTECTED information: consult Data Strategy and Governance (datagovernance@uq.edu.au) to ensure all security risks are managed correctly. Further risk assessments may be required and Legal Services can also assist if needed.

Create, Capture and Classify

(20) Individuals must comply with the following requirements (as relevant):

a. Ensure data is accurate, valid and complete at the time of capture and creation to maintain data quality.
b. Identify and record metadata (such as the individual who created the data) where possible.
c. Classify data and information at the time of creation or capture, according to the Information Security Classification Procedure and direction from the relevant Information Steward.
d. Any collection of personal information must comply with the Privacy Management Policy and Privacy Management Procedure. For more information, contact the RTI and Privacy Office (rtip@uq.edu.au)
e. Consider the University's moral and ethical obligations at the time of data collection (e.g. transparent disclosure of information about data collection, processing, and use). View UQ's Enterprise Data Ethics Framework.
f. Only create or capture data required for a legitimate and defined University purpose, to minimise the collection of personal information and/or SENSITIVE or PROTECTED information.
g. For Microsoft Office 365 documents and emails, ensure the correct sensitivity label is applied in accordance with the relevant information security classification. If not updated, the 'OFFICIAL' label will be applied by default. Read more about sensitivity labels.

Store and Secure

(21) Individuals must comply with the following requirements (as relevant):

Classification	Handling requirement
All	• Remove access to UQ information and systems when they are no longer required, or when an individual leaves UQ, changes their role, or ends their partnership or affiliation with UQ. View the departure checklist for more information. • Set secure passwords - read UQ's password guidelines. • Store UQ information in UQ-approved IT systems to ensure regular backups. Visit the Where to store files and information web page for guidance. – Ensure that appropriate access controls are in place, commensurate with the nature and sensitivity of the information. – Certain research data may be saved to local hard drives if they are being regularly and automatically backed up. Read more about backups. • Avoid unnecessary duplication of data across IT services, devices, and storage locations, including hard copies. • Store records in approved record keeping systems in alignment with the Records Management Procedure. • Do not use USB drives and portable hard drives unless they are encrypted. • Follow cyber security best practice – visit the stay cyber safe web page for more details. • Use UQ-approved online collaboration tools (e.g. UQ RDM, SharePoint and Microsoft Teams). Assign at least two (but no more than is necessary) administrators who must ensure access and permissions are set based on business need. • Report actual or suspected data loss or breaches (including lost or stolen devices) as soon as possible via UQ's cyber security website or by calling ITS support.
PUBLIC	• Restrict write access based on business need. PUBLIC information may be read by anyone but doesn't need to be published. • Collaboration space administrators must review write access annually.
OFFICIAL	• Restrict write access based on business need (e.g. specific teams). Where possible and appropriate, restrict read access based on business need. • Collaboration space administrators must review read and write access every 12 months.
SENSITIVE	• Restrict write access based on strict business need (e.g. specific individuals or groups). Where possible and appropriate, restrict read access based on strict business need. • Collaboration space administrators must review read and write access every six months. • Ensure hard copy information is stored in a locked cabinet when not being used.
PROTECTED	• Restrict write access based on very strict business need (e.g. only the individuals required). Where possible and appropriate, restrict read access based on very strict business need. Staff screening may be required. • Collaboration space administrators must review read and write access every three months. • Use file-based encryption where possible. Store back-up encryption passwords in UQ's enterprise vault. • Where possible, use online files rather than copying/downloading them to local storage for processing. Do not use web-based file shares which synchronise files to local storage (e.g. OneDrive). Delete any local copies of files when they are no longer required. • Ensure hard copy information is stored in a locked cabinet when not being used.

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.

Classification	Handling requirement
Supporting information: • Endpoint Security Standard • Application Security Standard • Data Security Controls Standard • Access and Privileges Management Framework • Authentication Framework • Network Security Controls Standard	

Manage and Maintain

(22) Individuals must comply with the following requirements (as relevant):

Classification	Handling requirement
All	• Notify Data Strategy and Governance (datagovernance@uq.edu.au) if an Information Leader, Information Domain Custodian or Information Steward is exiting their current role. Ensure an acting Information Leader, Information Domain Custodian or Information Steward is appointed to ensure information governance and management responsibilities are met during the transition. • Information Stewards must ensure that data and information within their entities are actively managed to ensure data quality, ongoing continuity of discovery and access (e.g. ensuring the relevant IT services hosting the information are serviced and supported appropriately), and compliance with UQ's privacy and information management requirements. • Technical Owners must review the information security classification of IT services (with support from Data Strategy and Governance) in alignment with the Application Security Standard.
PUBLIC and OFFICIAL	• Proactively review the information security classification of documents, data sets and collaboration spaces as information or requirements change, or at least every 36 months.
SENSITIVE	• Proactively review the information security classification of documents, data sets and collaboration spaces as information or requirements change, or at least every 24 months.
PROTECTED	• Proactively review the information security classification of documents, data sets and collaboration spaces as information or requirements change, or at least every 12 months.
Supporting information: • Application Security Standard • Access and Privileges Management Framework • Information Security Classification Procedure	

Share and Reuse (transmission)

(23) Individuals must comply with the following requirements (as relevant):

Classification	Handling Requirement
All	• A data sharing agreement may be required to access or use corporate UQ data. This includes the use of data for integration, analytics, or reporting. Visit the Request access to data page. • Sharing data outside UQ requires approval from the relevant Information Steward (a data sharing agreement may be used to facilitate this approval). Ensure the agreement or contract includes data handling and security provisions that align with UQ's policies, procedures and internal security controls. Engage with Data Strategy and Governance (datagovernance@uq.edu.au) before proceeding. • Personal information may only be used (i.e. within UQ) or disclosed (i.e. outside UQ) in accordance with the Privacy Management Policy. Except where explicitly allowed for under the Privacy Management Policy, any disclosure or secondary use of personal information may require a privacy impact assessment (see clauses 14-15). • UQ data should be used in an ethical and responsible manner, including any sharing or reuse. Visit the data ethics web page or read the Enterprise Data Ethics Framework. • Validate the identity of individuals receiving UQ data (e.g. check UQ email, check via phone call) and their authorisation to receive the data. • Only share or transfer information using UQ-approved IT services. Read more about where to store files and information. • Only share data (internally or externally) if required for a legitimate and defined University purpose or requirement, to minimise the disclosure of personal information and/or SENSITIVE or PROTECTED information. • Do not print data unless there is a genuine requirement to do so.
SENSITIVE and PROTECTED	• Only share research data using IT services approved to handle SENSITIVE and PROTECTED data, in accordance with ethics approvals. Read more about where to store files and information. • If transporting large data sets using physical storage devices, ensure devices are encrypted and passwords are shared securely with the receiver. • Do not print data unless there is a genuine requirement to do so. If required, do not use printers in low security areas or connected to general office networks. Use managed printers that require staff to log in at the printer to collect printouts.
Links: • Records Management Procedure • Data Security Controls Standard • Network Security Controls Standard • Authentication Framework	

Retain and Archive

(24) Individuals must comply with the following requirements (as relevant):

a. Retain data and information only for as long as UQ has a business requirement to retain it (including any records retention requirements). Dispose of data and information if no longer required.
b. Retain and archive records in compliance with the Records Management Procedure (see retention schedules) and the Public Records Act 2023 (Qld).
c. Contact the relevant Information Steward to recommend the retention or archival of high risk, high value, vital and permanent retention records. Information Stewards will review and seek approval from the appropriate Information Domain Custodian.
d. If decommissioning a system that contains UQ data, consult Data Strategy and Governance (datagovernance@uq.edu.au) regarding any decisions to retain, transfer or dispose of the data.
e. Comply with research data retention requirements in the Australian Code for the Responsible Conduct of Research.

Dispose and Destroy

(25) Individuals must comply with the following requirements (as relevant):

a. The relevant Information Domain Custodian must endorse the destruction of University records within their domain. However, the final approval must be obtained from the Senior Manager, Data Strategy and Governance, in compliance with the Records Management Procedure.
b. Ensure data is disposed of securely, including all copies, backups and devices (if required). Submit an IT support request regarding device redeployment and disposal.
c. Printed documents and other information in a physical format (e.g. tapes, CDs) must be disposed of using approved secure shredding and destruction services.

Section 4 - Roles, Responsibilities and Accountabilities

(26) Key roles and responsibilities relevant to this Procedure are outlined in the subsections below. Refer to the Information Governance and Management Framework for a comprehensive list of information governance and management roles.

Vice-Chancellor

(27) The Vice-Chancellor is accountable for ensuring the collection and management of UQ's information and records in accordance with relevant legislative, regulatory and policy obligations.

Chief Information Officer (CIO)

(28) The CIO is accountable for developing, maintaining and implementing information management capabilities, policies, procedures and technical standards to protect UQ's information.

Information Domain Custodians

(29) Information Domain Custodians are responsible for the following (for their information domain/s):

a. defining business area specific (e.g. research) operating procedures and controls to ensure legislative and policy obligations are met, and to ensure the confidentiality, integrity, availability and appropriate and ethical use of information;
b. approving privacy impact assessments;
c. approving access policies (including any changes) for their information domains;
d. approving requests to retain or archive high risk, high value, vital and permanent retention records; and
e. endorsing disposal requests for records for approval by the Senior Manager, Data Strategy and Governance.

Information Stewards

(30) Information Stewards are responsible for the following (for the information entity/entities they are assigned to):

a. providing advice and making decisions regarding day-to-day management of information;
b. conducting privacy impact assessments and submitting approved assessments to the RTI and Privacy Office;
c. setting and/or endorsing an overall information security classification for each information entity;
d. reviewing and recommending decisions regarding records disposal and the retention or archiving or high risk, high value, vital and permanent retention records;

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.

e. reviewing and approving data access requests (e.g. data sharing agreements); and
f. applying UQ-wide policies and procedures and business area specific (e.g. Research) operating procedures and controls to ensure legislative and policy obligations are met.

Technical Owners

(31) The Technical Owner is the staff member responsible for the ongoing technical management of a service or asset (e.g. information system).

(32) Technical Owners are responsible for:

a. supporting Information Stewards to implement technical controls outlined in this document and associated procedures and standards. Visit the IT procedures, frameworks and standards library for more information; and
b. assisting Information Stewards to conduct privacy impact assessments for the implementation of new systems or business processes (or changes to existing systems or processes) as required.

Senior Manager, Data Strategy and Governance

(33) The Senior Manager, Data Strategy and Governance is responsible for:

a. maintaining and implementing this Procedure;
b. escalating high-rated risks to UQ committees requiring resolution as required; and
c. approving records disposal requests.

Data Strategy and Governance Team

(34) The Data Strategy and Governance team supports the Senior Manager, Data Strategy and Governance to maintain and implement this Procedure. The team is also responsible for:

a. reporting to UQ committees on information management compliance as required (including reporting on records management and data sharing internally and externally);
b. facilitating data sharing agreements (DSAs) and maintaining a register of DSAs;
c. providing advice regarding data handling (including during projects);
d. advising on the management, treatment, and preservation of vital, high-risk, high-value and permanent retention records;
e. maintaining and implementing records management procedures;
f. delivering training and awareness regarding data handling principles and processes; and
g. providing training and support for Information Domain Custodians and Information Stewards.

Right to Information and Privacy Office (RTI and Privacy Office)

(35) The RTI and Privacy Office is responsible for:

a. providing advice and leadership regarding privacy compliance, privacy impact assessments and the management of personal information;
b. providing advice to business units on notifying individuals affected by privacy breaches; and
c. maintaining records of approved Privacy Impact Assessments.

UQ community

(36) Members of the UQ community are responsible for:

a. complying with this Procedure (and any business area-specific information management procedures) to handle the University's information ethically and securely;
b. reporting real or suspected data breaches or cyber security incidents via the cyber security webpage;
c. reporting lost or stolen devices containing UQ information to IT support;
d. using UQ-approved IT services and consulting ITS regarding the use of new IT services to handle data;
e. seeking approval before destroying UQ records in compliance with the Records Management Procedure; and
f. managing and reviewing access permissions (e.g. read and write access) for documents and collaborative spaces (e.g. SharePoint and Teams) they manage.

Section 5 - Monitoring, Review and Assurance

(37) The Data Strategy and Governance team will:

a. provide training and deliver awareness initiatives to the wider UQ community as required, to improve data literacy and awareness across UQ;
b. report on information and records management risk and compliance to the IT Policy, Risk and Assurance Committee (IT PRAC) quarterly and to other UQ committees as required, in alignment with the IT Governance and Management Framework;
c. maintain and update the information entity catalogue to ensure its accuracy; and
d. review and update this Procedure as required to ensure its accuracy.

Section 6 - Recording and Reporting

(38) The Data Strategy and Governance team maintains UQ's information entity catalogue which records:

a. information domains and information entities;
b. Information Leaders, Information Domain Custodians and Information Stewards assigned to each business area, domain and entity (respectively); and
c. information security classifications for each UQ information entity (as a minimum, UQ information entities will be assigned a classification based on the highest classification rating of the information held).

(39) The Data Strategy and Governance team also maintains a register of all submitted data sharing agreements.

(40) The RTI and Privacy Office maintains a register of approved Privacy Impact Assessments (PIAs) and is responsible for (where applicable) reporting privacy breaches to the relevant Information Commissioner or privacy regulator. The RTI and Privacy Office also provides management with an annual report on UQ's compliance with the Information Privacy Act 2009 and other relevant privacy laws.

(41) Information management roles and responsibilities should be captured as a research data management record in UQ RDM. Research data management plans should also be stored in UQ RDM where possible.

Section 7 - Appendix

Key contacts

(42) Individuals can seek advice from the following groups as required:

a. Information Stewards: advice regarding classifying information, local data handling processes, data access

requests, and appropriate and ethical use of information.

b. Data Strategy and Governance (datagovernance@uq.edu.au): advice regarding information governance and management, data handling requirements, data access requests, UQ-approved information systems, records retention requirements, UQ-approved record keeping systems, and records disposal or transfer.
c. ICT Procurement: advice regarding procuring new IT systems, services and software.
d. Right to Information and Privacy Office: advice regarding personal information (e.g. consent, collection notices) and privacy, privacy impact assessments.
e. Cyber security: advice regarding cyber security risk assessments, security controls, cyber security incidents, additional security requirement relating to third party agreements.
f. ITS relationship managers: advice regarding new IT services, key changes to existing IT services, integrations, projects with IT requirements. Read more: Projects with IT Requirements.

Definitions

Term	Definition
Data	refer to the Information Management Policy.
Information	refer to the Information Management Policy.
Record	refer to the Information Management Policy.
UQ community	refer to the Information Management Policy.
Information entity	refer to the Information Management Policy.
Information domain	refer to the Information Management Policy.
Personal information	refer to the Privacy Management Policy.
Write access	access to edit information.
Read access	access to view information.
Access policy	a policy specifying who can create, access or modify information for a particular domain. See the Access and Privileges Management Framework for more information.
Data breach	where data is lost, or accessed or disclosed without authorisation, either accidentally or due to malicious activity.

Status and Details

Status	Historic
Effective Date	9th January 2024
Review Date	9th January 2027
Approval Authority	Chief Information Officer
Approval Date	9th January 2024
Expiry Date	28th August 2025
Policy Owner	Zoran Sugarevski Chief Information Officer
Enquiries Contact	Information Technology Services

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to refer to The University of Queensland's Policy and Procedure Library for the latest version.