What is the **Data Handling Procedure?**

The *Data Handling Procedure (DHP)* **outlines handling requirements** for all **data (structured and unstructured), information, and records** in digital or electronic formats at UQ. DHP is quite **technical** in nature, with much of the content **directed towards** those who **manage storage systems**. This one-pager gives a simple **overview of the key aspects** of the DHP that **need to be considered by staff in everyday work.**

Key Framework

Data handling is the **process of storage, archival, planning, creation, management, or disposal** of the various types of data used at UQ, using the **correct level of security protocols and permissions**.

UQ uses an **information management lifecycle** (diagram overleaf). Key considerations for general staff in their everyday work for each stage are outlined below. For more information, read the Data Handling Procedure.

Note: 'plan and design' should be reviewed at every subsequent stage.

Plan and design	Data must be assigned an appropriate **Domain, Information Domain Custodian**, and **Information Steward**, as per the Information Governance and Management Framework. If the requirements **can't be met**, please **contact the Data Governance team** for assistance, or to apply for an exemption. For **SENSITIVE** and **PROTECTED** data, a **PIA and risk assessment** should be conducted. Data retention and disposal **requirements must be understood**, so they can be subsequently **applied appropriately**.
Create, capture and classify	Data quality is the **responsibility of the creator,** and must comply with policies and procedures. The **creator** must be **identified and recorded**, where possible.
Store and secure	The **principle of 'least privilege' should be followed**, with personnel only granted access to the data required to execute their responsibilities. **Data should be backed up**, using **methods appropriate to its classification**, and useable for the detection of unauthorised changes in the production copy, as well as recovery from disasters. For **OFFICIAL - INTERNAL, SENSITIVE, and PROTECTED data**, **local copies should not be made to portable devices**, remaining on UQ managed endpoints (e.g. SharePoint).
Manage and maintain	For a **detailed table of when reviews, audits, and testing should be done**, according to classification, click here.
Share and reuse	For **SENSITIVE and PROTECTED** data, where available, **dedicated systems** must be used for sharing and transmission, **rather than ad-hoc methods** (e.g. email, print outs). Additionally, **data transferred in bulk via portable disks, devices**, and other media **must be encrypted**, with keys transferred separately, and not reused for subsequent transfers. This should **also be done for OFFICIAL – INTERNAL data**, where possible. Read more here.
Retain and archive	The **Information Steward** must **approve the retention and archival of data and records**. Data must be accessible, usable, and readable, through the whole archiving period.
Dispose and destroy	Follow the Destruction of Records Procedure. The **Information Domain Custodian** and **Information Steward** must **endorse the destruction of records**, with **final approval from the UQ Records Manager**, and the process and approvals of data records documented and captured into the Enterprise Document and Records Management System.

For further information contact Data Strategy & Governance

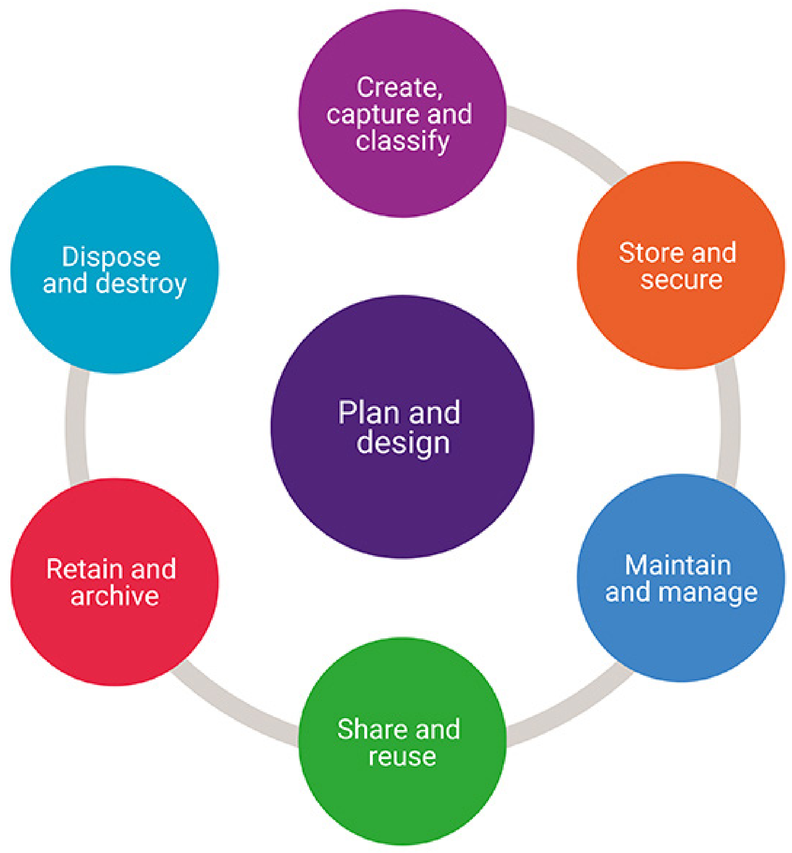
data.uq.edu.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Where to **store your digital files**

Why the Data Handling Procedure Matters

At UQ, information is a **core strategic asset**, and needs to be **managed accordingly** through its lifecycle. Adherence to data handling procedures assists in **maintaining security standards**, **integrity of information**, and **safety** of both work and the University.



Key definitions

Information security classification Details requirements for information, both digital and/or physical, at UQ, providing a consistent approach. Read more here.

Information service providers Individuals that provide support to embed and implement governance controls and processes – includes technical teams that provide support and manage access.

RAMS (Records Advisory and Management Services) Located within ITS, responsible for the management of record keeping systems, developing policies, and providing advice.

PIA (Privacy Impact Assessment) An assessment of a project that identifies the impact it may have on the privacy of individuals, recommending how to minimise or eliminate impact. Read more here.

Information asset register A comprehensive outline of information gathered by UQ (including teaching and learning activities, library catalogue, student residence records).

Records register Personal information about students, staff, and other clients that is collected, stored, and used (includes financial records, information technology systems that store personal information).

Information domain A category or theme where information can be identified and managed.

Information domain custodian Overseer that is responsible for defining domain-specific procedures and rules to ensure quality, security, privacy, and accessibility of information throughout its lifecycle.

Information steward Responsible for the quality, integrity and use of the information assets within their Information Sub-Domain. Read more here.

For further information contact Data Strategy & Governance

data.uq.edu.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE