

# What is the Data Handling Procedure?

The *Data Handling Procedure (DHP)* outlines handling requirements for all **data, information, and records** in digital or electronic formats at UQ.

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](#). Key considerations for general staff at each stage are outlined below. For more information, read the [Data Handling Procedure](#). **Note: ‘plan and design’ should be reviewed at every subsequent stage.**

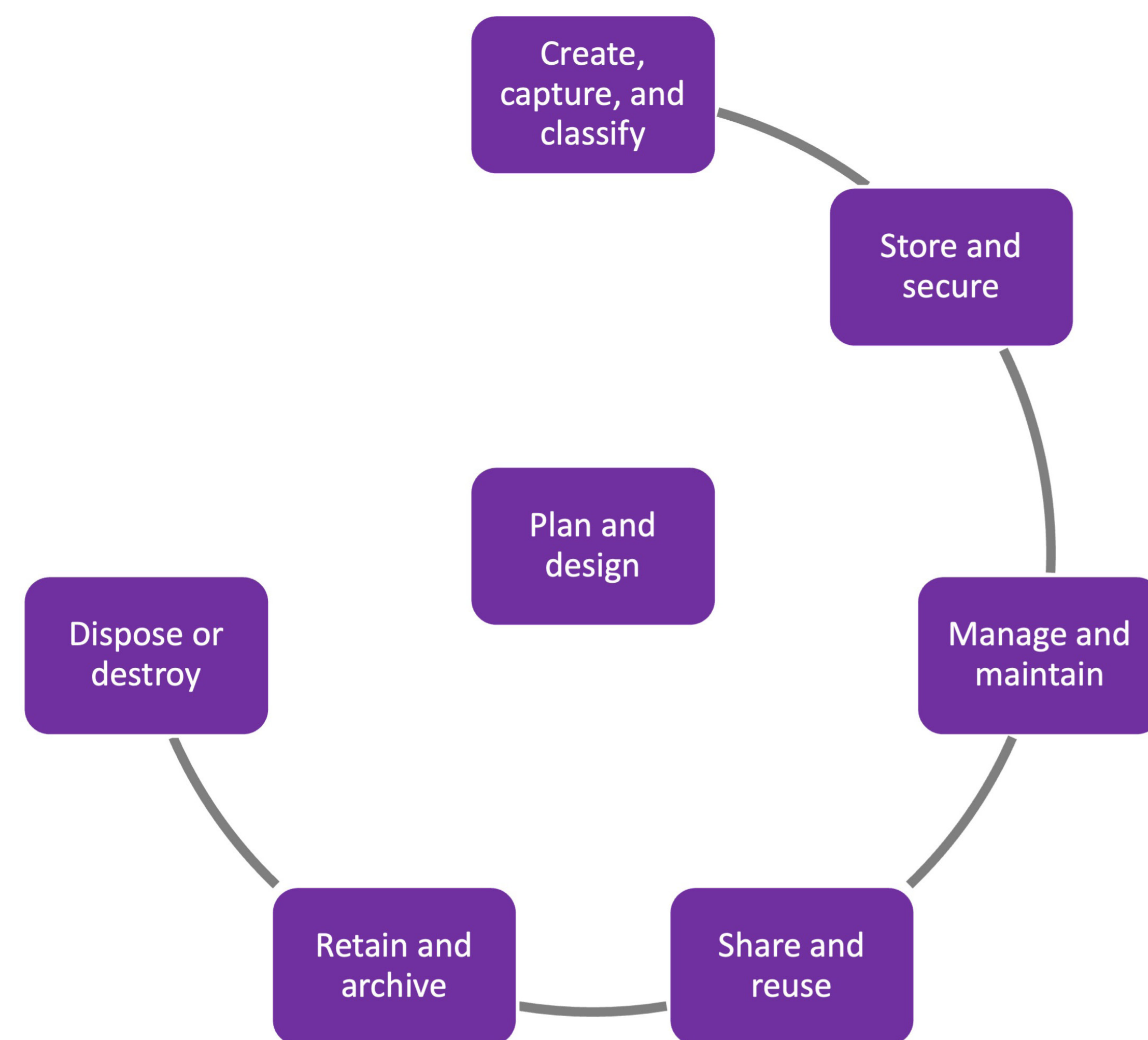
<i>Plan and design</i>	Data must be assigned an appropriate <b>Domain, Information Domain Custodian</b> , and <b>Information Steward</b> , as per the <a href="#">Information Governance and Management Framework</a> . If the requirements <b>can’t be met</b> , please <b>contact the Data Governance team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



# Key definitions and data roles

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 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 Entity. [Read more on the Data at UQ website.](#)

For further information contact Data Strategy & Governance

[data.uq.edu.au](http://data.uq.edu.au)