Appendix 2: Information Governance Instruction Manual

Introduction

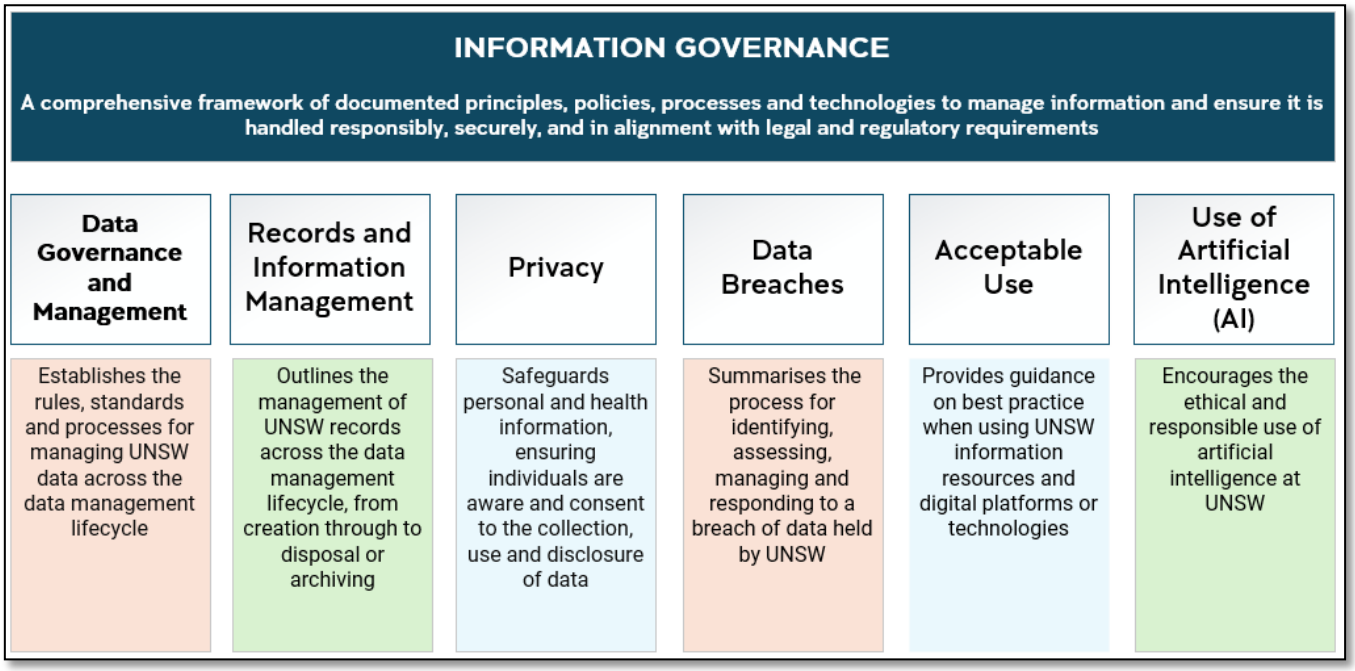
UNSW is committed to maintaining the security, integrity and appropriate management of its data, information and records.

This is achieved principally through the Information Governance Policy, established in February 2025 to amalgamate and replace individual policies and procedures for privacy, data breaches, data management, research data management, recordkeeping, and acceptable use of information resources.

Related standards and guidance are collected in this Instruction Manual.

UNSW defines information governance as a 'comprehensive framework of documented principles, policies, processes and technologies to manage information and ensure it is handled responsibly, securely, and in alignment with legal and regulatory requirements.'

Information governance includes data governance and management, records and information management, privacy, data breach management, acceptable use of information resources, and use of artificial intelligence (AI).



Scope

The Information Governance Policy and Instruction Manual apply to all data, information and records collected, created and/or used at UNSW, including research data.

Where an element of this Instruction Manual applies specifically or differently to research data, this requirement has been highlighted.

Purpose

The purpose of this Instruction Manual is to:

- provide a comprehensive set of instructions for the (i) management of data, information and records, and (ii) use of UNSW information resources, digital communication platforms/technologies and artificial intelligence (AI) systems or tools, in accordance with the Information Governance Policy
- assist the University to comply with applicable laws, regulations, standards and contractual obligations in relation to information governance.

(For ease of reference, the relevant clauses of the Information Governance Policy are footnoted throughout this Manual.)

Governance[1]

Information Governance Steering Committee

Once established, the Information Governance Steering Committee (IGSC) will oversee UNSW-wide information governance and provide oversight and assurance of related strategic initiatives to protect data, information and records across UNSW.

The proposed Terms of Reference for the IGSC are available here.

Data Governance and Management Committee

The Data Governance and Management Committee will replace the existing Data & Information Governance Steering Committee. Once established, it will oversee the governance and management of data (non-research data) on behalf of the IGSC.

Research Data Governance and Management Committee

The Research Data Management Committee will replace the existing Research Data Management Steering Committee. Once established, it will oversee the governance and management of research data on behalf of the IGSC.

[1] See clauses 7.1 – 7.3 of the Data Governance and Management Procedure in the Information Governance Policy.

Section 1: Data Governance and Management

Data governance

Data governance is the organisation and implementation of policies, procedures, structure, roles, and responsibilities, which outline and enforce rules of engagement, decision rights, and accountabilities for the effective management of data and information assets.

Data management

Data management is a group of activities relating to the planning, development, implementation and administration of systems for the acquisition, use, storage, security, retrieval, dissemination, archiving and disposal of data.

Key data management activities include:

- data policy development
- data ownership
- metadata compilation
- data lifecycle control
- data quality, and
- data access and dissemination.

Data management embraces all forms of data including simple paper forms, the contents of relational databases, multimedia datasets such as images, and research data.

Effective data management enables good stewardship of public resources and responsible communication of research results and is an essential governance practice for the modern world to protect data and information assets.

Storing the right data in the right place protects staff, teaching and research work, and the University's reputation. Failing to do so may result in the recreation of documents, redoing of experiments, paying to repeat procedures, hours of administrative cleaning-up and searching through multiple backup tapes, or having to retract a published paper.

UNSW data domains[2]

The responsibility for ascribing a non-research data domain rests with the relevant Data Executive.

Research data domain
The responsibility for distribution of roles within the research data domain rests with the Research Data Management Steering Committee.

[2] See clauses 1.3 – 1.4, 8.3 – 8.5 of the Data Governance and Management Procedure in the Information Governance Policy.

Data management plans[3]

Data management plans outline how data is collected, organised, managed, stored, secured, and shared.

A data management plan is a living document that should be amended to reflect changes in the data and the details (or metadata) of data as they arise.

There are two types of data management plans at UNSW:

(i) data management plans for non-research data. A template data management plan can be accessed here.
(ii) research data management plans (refer to ResToolkit).

The Data Custodian is responsible for submitting a data management plan for each of their data domains at the beginning of the data lifecycle and updating the plan throughout each phase of the data lifecycle.

[3] See clauses 1.2 – 1.7, 2.1, 2.12, 3.8, 4.3, 5.16 of the Data Governance and Management Procedure in the Information Governance Policy.

Research data management plans (RDMP)[4]

An RDMP is a mandatory requirement for those undertaking research to record metadata about research projects or research activities in ResToolkit. An RDMP also enables researchers to provision storage on platforms such as Data Archive, OneDrive, and Teams.

There are up to 3 types of research projects in ResToolkit, categorised by the source of the original project record:

- *Grant-funded projects (InfoEd):* These projects are grant records from InfoEd listing your name as either the Chief Investigator or member of the project. RDMPs created from InfoEd projects will have certain fields pre-filled from InfoEd.
- *HDR projects (HDR):* These projects are records from the Graduate Research Information System (GRIS) listing you either as the Supervisor, Co-supervisor or HDR candidate of the HDR project. RDMPs created from HDR projects will have certain fields pre-filled from GRIS.
- *Manual Projects (Manual):* These projects are not linked to a Grant-funded project or HDR Candidature.

The Data Custodian is responsible for oversight of the RDMP in ResToolkit. The Data Custodian is required to review and update the RDMP as change occurs (i.e. researchers joining or leaving) throughout the lifecycle of the research project or research activity.

Creating your RDMP

The ResToolkit Getting Started – Research Data Management Plan page provides guidance on how to create (and complete the mandatory fields of) an RDMP.

The IT Service Desk or RDM@UNSW provide support for researchers with questions or concerns about commencing and completing an RDMP.

Data Ethics Guideline[5]

The Data Ethics Guideline sets out principles, practices and tools for ethically managing (non-research) data.

Data Custodians are responsible for ensuring that management of non-research data created or collected in their data domains comply with the Data Ethics Guideline as well as UNSW's Privacy Management Plan, relevant UNSW Privacy Statements, codes and guidelines, and third-party agreements.

[4] In the Data Governance and Management Procedure of the Information Governance Policy, see clause 1.5 and the callout box under clause 3.8 entitled "Research Data".
[5] See clauses 2.3 and 4.2 of the Data Governance and Management Procedure in the Information Governance Policy.

The Data Ethics Guideline is not applicable to research data. Information about research data ethics requirements can be found on the Research Ethics & Compliance Support page.

Data Quality Guideline[6]

The Data Quality Guideline sets out principles, practices and tools for achieving fit-for-purpose data.

Data Custodians are responsible for ensuring that any data being created or collected in their data domains comply with the Data Quality Guideline.

The Data Quality Guideline is not applicable to research data.

Indigenous data

The Global Indigenous Data Alliance (GIDA) states that "Indigenous data, in general, comprise data, knowledge, and information that relate to Indigenous Peoples at both the individual and collective level, including data about lands and environment, people, and cultures".[7]

UNSW is committed to the GIDA CARE Principles for Indigenous Data Governance (CARE principles):

- **Collective Benefit:** Data ecosystems shall be designed and function in ways that enable Indigenous Peoples to derive benefit from the data.
- **Authority to Control:** Indigenous Peoples' rights and interests in Indigenous data must be recognised and their authority to control such data be empowered. Indigenous data governance enables Indigenous Peoples and governing bodies to determine how Indigenous Peoples, as well as Indigenous lands, territories, resources, knowledges and geographical indicators, are represented and identified within data.
- **Responsibility:** Those working with Indigenous data have a responsibility to share how those data are used to support Indigenous Peoples' self-determination and collective benefit. Accountability requires meaningful and openly available evidence of these efforts and the benefits accruing to Indigenous Peoples.
- **Ethics:** Indigenous Peoples' rights and wellbeing should be the primary concern at all stages of the data lifecycle and across the data ecosystem.

As this is an emerging area for UNSW, guidance on Indigenous (including Aboriginal and Torres Strait Islander) data will evolve in consultation with the Pro Vice Chancellor (PVC) Indigenous and Indigenous Reference Group.

[6] See clauses 2.3, 3.3, 4.2 and 8.3 of the Data Governance and Management Procedure in the Information Governance Policy.
[7] See Indigenous Data | ARDC

Aboriginal and Torres Strait Islander research data[8]

In addition to the GIDA CARE principles, UNSW is committed to the *AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research* (AIATSIS Code).

For the purposes of this Code, Aboriginal and Torres Strait Islander research should be understood as research that concerns or impacts Aboriginal and Torres Strait Islander peoples in any of the following ways:

- The research is about Aboriginal and Torres Strait Islander peoples, societies, culture and/or knowledge, Aboriginal and Torres Strait Islander policies or experience.
- The target population is Aboriginal and Torres Strait Islander individuals, groups, communities or societies.
- The target population is not explicitly Aboriginal and Torres Strait Islander individuals or communities, but the research population includes a significant number of Aboriginal and Torres Strait Islander people.
- Aboriginal and/or Torres Strait Islander people have been incidentally recruited and researchers wish to do separate analysis of Indigenous-specific data.
- There are Aboriginal and Torres Strait Islander individuals or communities contributing to the research.
- There is new or pre-existing data related to Aboriginal and Torres Strait Islander peoples being used in the research.
- The research concerns Aboriginal and Torres Strait Islander peoples' lands or waters.

The Indigenous Cultural and Intellectual Property (ICIP) principles and procedures are also in development and will provide further support to researchers to understand their obligations in relation to Aboriginal and Torres Strait Islander research data.

For further information on the ethical requirements in relation to human research see Research within Aboriginal & Torres Strait Islander Communities.

Data collection

Guidance on the appropriate capture and collection of records in a UNSW System of Record can be found in **Section 2: Records and Information Management** of this Manual.

[8] Refer to the same sources as non-research Aboriginal and Torres Strait Islander data.

Research data collection[9]

Research data collection (also known as creation or generation) is the process of gathering original and valuable information to validate or reproduce findings in a research project. The response to a particular research question is based on the analysis of research data. In general research data collection is done using generic file systems, but in some instances researchers may use specific research systems or instruments.

Capturing and Managing Data from Surveys

UNSW approved storage tools for online survey or data collection

Online platforms are increasingly replacing paper-based data collection tools because of their efficiency and ability to store collected data.

Researchers collecting research data and materials via data entry or surveys should use UNSW approved data collection and storage tools where possible.

The supported platforms for research surveys and data collection at UNSW are REDCap and Qualtrics.

Online interview collection and storage tools

- **Microsoft Teams**
- **Zoom**

Microsoft Teams and Zoom can record and collect data in different ways. To ascertain which storage platform is right for you click here - Storage (sharepoint.com)

Third-party unsupported tools

Researchers who wish to use an external or third-party research tool should first ensure that the tool complies with UNSW's Cybersecurity policies. For assistance in finding and assessing external tools, contact rdm@unsw.edu.au

Metadata[10]

Metadata is data that describes other data, providing a structured reference that helps to sort and identify attributes of the information it describes, such as structure of data, data definition etc.

Metadata is captured and managed in different ways across the life of a project, depending on which phase the project is in. These phases are often described as part of a 'data management lifecycle'. For metadata capture and management, consider the following phases:

[9] In the Data Governance and Management Procedure of the Information Governance Policy, see the callout box under clause 2.7.
[10] See clauses 1.7 and 4.4 of the Data Governance and Management Procedure in the Information Governance Policy.

- **Plan and design:** Review established metadata schemas and understand metadata requirements.
- **Create, collect and classify:** Choose and implement metadata schema or templates that align with business requirements.
- **Organise, store and secure:** Document and communicate the value of metadata to stakeholders.
- **Manage and maintain:** Evaluate the ongoing quality of metadata.
- **Share and (re)use:** Provide staff with training and support to create, access, use, reuse and share metadata in accordance with UNSW policy.
- **Retain:** Use metadata to determine the retention period of the data it describes.
- **Dispose and destroy:** Consult with the relevant users when data that the metadata describes is being disposed, destroyed or migrated.

The Data Custodian is responsible for:

- describing, documenting and recording metadata in a Data Management Plan as soon as metadata is created or collected
- recording the consented uses of data within the metadata during data collection
- determining levels and types of metadata requirements/schemas in line with business requirements, user needs and technical capabilities
- ensuring metadata is maintained in a format that is exportable/consumable by any enterprise data governance platform or tool that is in place in the future. Some of the common formats supported include Json, Excel, CSV, XML, Direct Data, and base connectivity
- measuring, monitoring and conducting quality assurance audits on metadata throughout the data management lifecycle, including through changes of systems and storage changes.

Data Custodians can contact the UNSW Cyber Security Team for more information about the management of metadata throughout the data lifecycle.

For guidance on Records and Information metadata, refer to **Section 2: Records and Information Management** in this Manual.

Metadata for Research Data [11]

Collection of metadata is important for many reasons, chiefly among them:

- visibility and credit
- transparency and robustness
- publisher and funder requirements

Data Custodians are responsible for organising, naming and describing their research data to ensure that it is findable, structured, and clearly recorded (in compliance with the Information Titling Guideline).

For more guidance on organising your research data see Data Organisation:

- File Naming Conventions
- File Versioning
- Metadata
- eNotebook (available to record metadata in the form of observations or notes)

The Metadata guide is available for researchers using the Data Archive.

Publishing metadata about research

For guidance on publishing research metadata see Data - Publishing strategy guide - Library guides at UNSW Library.

Data classification[12]

Data classification is a framework for assessing data sensitivity measured by the adverse business impact a breach of the data would have upon the University. The classifications have been created to help the University community effectively manage information.

To ensure UNSW data is kept secure, the data must be classified and then only used or stored in applications, systems or platforms that have the correct level of data protection.

Data classification applies to:

- all data created, collected, used, stored or processed at UNSW
- all University employees, affiliates, vendors, consultants/contractors, etc.
- handling of University data, information and records in any form (paper, digital text, image, audio, video, microfilm, etc.) during conducting University business (administrative, financial, education, research or service).

There are **five** levels of data classification at UNSW. These classifications reflect the level of damage done to the organisational interest and individuals from unauthorised disclosure, or compromise of the confidentiality, of UNSW data.

[11] In the Records and Information Management Procedure, see the callout box under clause 4.2 entitled "Research Data".
[12] See clauses 2.8 – 2.12 of the Data Governance and Management Procedure in the Information Governance Policy.

All data at the University shall be assigned one of the following classifications:

Data classification	Description	Example Data Types
HIGHLY SENSITIVE	Data, that if breached owing to accidental or malicious activity, would have a high impact on the University's activities and objectives. The intended audience for data with this classification is from a restricted UNSW organisational unit or external perspective. Dissemination of this data is based on strict academic, research or business need	Data subject to regulatory control Medical • Individually identifiable health information created or received by a health care provider • Employee health records • Student care and health records Children and young persons (under 18 years) Passport, bank account or credit card details, Driver's licence, Visa number, Medicare number, Tax File Number zID password Physical and cyber security data Research data (containing identifiable personal/health data)
SENSITIVE	Data, that if breached owing to accidental or malicious activity, would have a medium impact on the University's activities and objectives. The intended audience for data with this classification is from a restricted UNSW organisational unit or external perspective. Dissemination of this data is based on strict academic, research or business need.	Personal information (other than that identified as HIGHLY SENSITIVE) Student and Employee HR data (other than that identified as HIGHLY SENSITIVE) Organisational financial data Exam materials and results Research data (containing personal data other than identifiable personal/health data)
RESTRICTED (formerly 'Private')	Data, that if breached owing to accidental or malicious activity, would have a low impact on the University's activities and objectives. The intended audience for data with this classification is from a broad UNSW organisational unit or external perspective. Dissemination of this data is based on academic, research or business need. This classification was formerly known as "PRIVATE" in previous versions.	Business unit process and procedure Unpublished intellectual property ITC system design and configuration information
	Data that does not form part of official duty.	

UNOFFICIAL		
PUBLIC	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and objectives. The intended audience for data with this classification is the general public.	Information in the public domain such as Faculty and employee directory information published on UNSW websites Course catalogues Published research data

Note: UNSW does not currently have the following classifications:

'**OFFICIAL**: Sensitive'
'**PROTECTED**'
'**SECRET**'
'**TOP SECRET**'

These classifications require specific Australian Government security clearances.

Most UNSW official information does not require increased security and may be marked **PUBLIC** or **UNOFFICIAL**. This should be the default position for newly created material unless there is a specific need to protect the confidentiality of the information.

Collections of diverse information should be classified at the most secure (that is, highest) classification level of any individual information component within the aggregated information.

The data classification checker assists data users and Data Custodians to identify the appropriate level of classification.

In addition to being assigned a classification, UNSW Digital Information must be assigned a Confidentiality Risk Rating based on the below table:

Digital Information	Low Confidentiality Risk Rating	Medium Confidentiality Risk Rating	High Confidentiality Risk Rating
Research related UNSW Digital Information	Consists of ONLY: ***Public*** UNSW Digital Information, OR ***Restricted*** or ***Sensitive*** UNSW Digital Information related to less than 1,000 individuals.	Consists of: ***Restricted*** UNSW Digital Information AND ***Sensitive*** UNSW Digital Information related to 1,000 to 10,000 individuals,	Consists of: ***Sensitive*** UNSW Digital Information related to more than 10,000 individuals, OR ***Highly Sensitive*** UNSW Digital Information related to more than or

		AND ***Highly Sensitive*** UNSW Digital Information related to less than 1,000 individuals, AND Has no other requirement for high security.	equal to 1,000 individuals, OR Has a contractual requirement, external partner, or regulatory requirement for high security.
All other UNSW Digital Information	Consists of ONLY: ***Public*** UNSW Digital Information, OR Less than 1,000 records of ***Restricted*** or ***Sensitive*** UNSW Digital Information.	Consists of: ***Restricted*** UNSW Digital Information AND Between 1,000 and 10,000 records of ***Sensitive*** UNSW Digital Information, AND Less than 1,000 records of ***Highly Sensitive*** UNSW Digital Information, AND Has no other requirement for high security.	Consists of: More than 10,000 records of ***Sensitive*** UNSW Digital Information, OR More than or equal to 1,000 records of ***Highly Sensitive*** UNSW Digital Information, OR Has a contractual requirement, external partner, or regulatory requirement for high security.

Classification of research data[13]

The Research Data Management Team have created a Research Data Classification Guide for classifying research data in accordance with the Data Classification Standard. The Guide is not intended to be exhaustive.

The classification of research data can change as it is altered throughout the research data life cycle. It is important to capture any changes to classification in the RDMP.

Data containing personal information requires care and consideration. The standard for identified data is defined as "an identifiable individual, or an individual who is reasonably identifiable". For data containing personal or sensitive identifiers, a common way to reduce risk is de-identification. Once researchers have de-identified research data containing personal or sensitive information, they can reclassify research data to reflect the lower risk rating and controls required. Both the Information Governance SharePoint and The Office of the Australian Information Commissioner provide information on de-identification.

For guidance on how to reduce the sensitivity of research data see Data Sensitivity & Classification (sharepoint.com)

Review and re-classification of research data

The Data Custodian, in conjunction with the researcher, is responsible for reviewing the classification of research data throughout the lifecycle of a research project or activity. If research data is re-classified (for instance once the sensitivity has been reduced) the new classification must be documented in the RDMP.

Researchers with questions about classifying their research data can contact RDM@UNSW.

Storage[14]

Guidance on the appropriate storage of digital information can be found in **Section 5: Digital communication platforms/technologies.** Information on the capture and storage of records in a UNSW System of Record can be found in **Section 2: Records and Information Management.**

[13] Ibid.
[14] See clauses 3.4 – 3.8 of the Data Governance and Management Procedure in the Information Governance Policy.

Research data storage[15]

UNSW offers researchers a range of supported data storage platforms, listed on the Research Data Management website. UNSW supported platforms have been evaluated against risk rating, security, backup and disaster recovery, storage limit, recovery from deletion and post-project data retention (amongst other criteria). The Data Storage Guide assists researchers in choosing the platform and software most appropriate for their data management requirements.

Overview of research data storage platforms

Supported UNSW Research Data Storage Solutions

1. **UNSW OneDrive & Teams** part of our Microsoft Office365 capability, is suitable for most research projects and is a great way to store and share data during a project. For more information, please go to: https://unsw.sharepoint.com/sites/LearnOffice365/SitePages/Products-at-a-glance.aspx

    a. N.B. There are limits on maximum individual file size (100gb) and other limits. For details see here: https://docs.microsoft.com/en-us/microsoftteams/limits-specifications-teams

2. **UNSW Shared Drive.** This is a mapped drive system accessible to all UNSW staff. These are recommended for documents and administrative data (excluding university records). For more information, please go to: https://www.unsw.edu.au/myit/services/storing-sharing-files/file-system-access-management-for-staff

3. **UNSW Data Archive** is an archival system designed to help researchers meet their obligations for long term management of research data, and provide a safe place to store research data long-term. For more information, please go to:

    https://www.dataarchive.unsw.edu.au/
    FAQs | UNSW Data Archive

4. **UNSW eNotebook** is an electronic notebook, this digital platform is designed to replace traditional paper research notebooks and provide researchers with a digital, collaborative, note-keeping tool. For more information, please go to: https://research.unsw.edu.au/enotebook

5. **Research Electronic Data Capture (REDCap)** is a widely used electronic data capture platform, designed to replace paper-based surveys and spreadsheet-based data capture systems. For more information, please go to: https://research.unsw.edu.au/redcap

6. **Qualtrics** is an easy-to-use, web-based platform for creating and distributing online surveys and is appropriate for any discipline of study. For more information, please go to: https://research.unsw.edu.au/qualtrics

7. **Version control – (GitHub and Azure Devops)**: Version control systems like GitHub and Azure Devops record changes to files over time, allowing researchers to go back to older versions, create new branches for experimentation. Version control is most useful for keeping track of programming code, large websites, documentation, and other collections of information. Using one of these cloud-based version control systems uploads copies of data to the service. These repositories can be private (only accessible by invited people), or Public, where the public can view the data. If public, ensure a license is applied to the data, and be aware that all files and their contents will be publicly available. For additional information about accessing UNSW-only GitHub repositories or signing up, see this website.

8. Adobe Cloud Storage is part of the Adobe Creative Cloud suite available to UNSW staff members, cloud storage is available. Some important details about this storage: https://www.it.unsw.edu.au/staff/software/adobe.html

External storage resources

UNSW supported storage platforms are a low-risk option for researchers storing their research data. However, researchers may wish to use external or third-party storage resources, which can carry some risk. Before using an external or third-party platform, researchers should ensure that the platform complies with UNSW's Cybersecurity policies. For assistance in finding and assessing external platforms, contact rdm@unsw.edu.au

Some external resources that have been used for UNSW research data include the following. Ensure that they are suitable for your data before using these platforms.

- National data platforms - these can be accessed directly or via Intersect and include med.data and omics.data (see http://www.intersect.org.au/data)
- Specialist secure options exist for sensitive medical data – please seek advice from RDM@unsw.edu.au

Note: Researchers must complete a RDMP to provision storage on Data Archive, OneDrive, and Teams tied to their research project.

Storage of physical research materials

UNSW provides a range of secure storage facilities for physical research materials:

- Surveying instrument museum | Surveying and Geospatial Engineering
- Museum of Human Disease | Faculty of Medicine & Health
- Biospecimen Services | UNSW Mark Wainwright Analytical Centre

[15] In the Data Governance and Management Procedure of the Information Governance Policy, see the callout box under clause 3.8 entitled "Research Data".

- BioRep - Health Precincts Biobank | UNSW Mark Wainwright Analytical Centre
- The John T. Waterhouse Herbarium | School of Biological, Earth & Environmental Sciences

Please contact the relevant faculty or shared facility for support and advice on the storage of physical research materials.

If it is not possible or practical to retain primary research materials then durable records of primary research materials (including metadata, transcripts, eNotebook, laboratory or field notes) should be retained instead.

Cold Storage

Certain research materials, including specimens or samples, must be handled in accordance with the Cold Storage Procedure.

For a more comprehensive list of digital storage options please visit the Data Storage and Tools page.

Contact for help, advice and inquiries

The Research Technology Data Support team can provide best practice advice on:

- help with supported systems
- data storage costs
- highly sensitive data (medical, social, cultural etc)
- large/sensitive data moves
- managing very large data sets.

For further advice on data systems or options to store data contact: rdm@unsw.edu.au

Further information about research data management, storage and tools can be found on the Research Infrastructure website.

Research data encryption[16]

Digital research data should always be stored in a stable format, encrypted if necessary, and regularly backed up to an external source.

In the UNSW Cyber Security Standard – Data Security S(3) data classified as being of a Medium or High Confidentiality Risk Rating must be stored encrypted at rest (including when backed up or archived). This encryption should follow Appendix A of the Standard - Approved Algorithms and Protocols. UNSW supported platforms such as OneDrive and Teams are already encrypted.

Once research data has been encrypted it can only be accessed by users with a 'key', preventing unauthorised access, data loss, and breaches. However, if a researcher loses the key, they could permanently lose access to their research data.

There are many encryption options available, when choosing researchers should consider their (and their collaborators) access needs, the operating system of their device, and whether the encryption can be supported by a recovery mechanism.

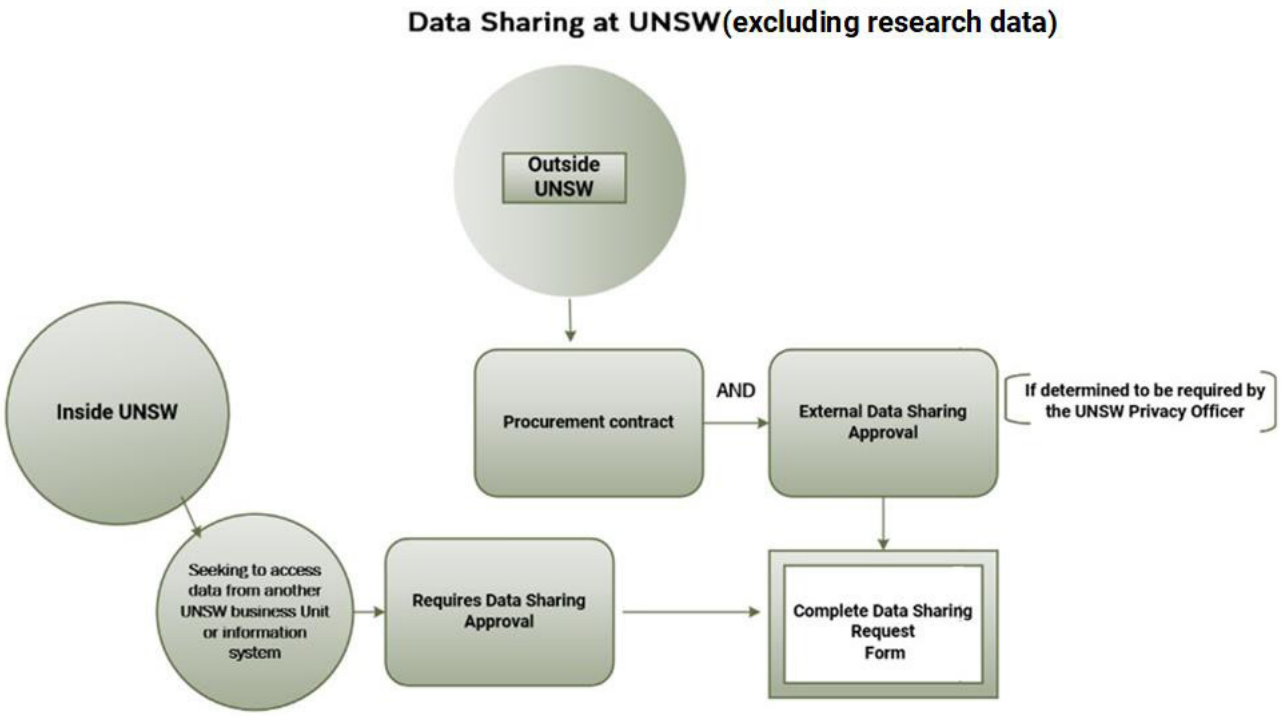
For guidance on encryption options, see File Encryption.

Data sharing[17]

Data can be shared if it has been classified as **UNOFFICIAL** or **PUBLIC**. Refer to the data classification table for examples of PUBLIC data.

Before accessing or using **RESTRICTED**, **SENSITIVE** or **HIGHLY SENSITIVE** data, most Data Users must obtain written permission from the relevant Data Custodian. Written permission is usually in the form of a data sharing approval.

[16] See clauses 2.9 – 2.11 of the Data Governance and Management Procedure in the Information Governance Policy.
[17] See clauses 5.1 – 5.6 of the Data Governance and Management Procedure in the Information Governance Policy.



Data sharing approvals for non-research data

There are five steps that are required to be taken to obtain a data sharing approval (DSA) for non-research data:

1. Planning ahead
2. Requesting the data
3. Confirming whether a DSA is needed
4. Gathering the information necessary to complete a request
5. Requesting a DSA.

Visit the DSAs in progress Confluence page for a list of data sharing approvals currently in progress at UNSW.

Planning ahead

Data Users should request a DSA as soon as possible because a DSA can take several weeks or more to draft and approve. This is due to factors such as:

- the complexity of the data request
- the information systems involved
- the need for related reviews such as a Cyber Security Vendor Assessment or Cyber Security Risk Assessment (CSRA)
- the availability of Data Custodians to review and approve the data approval
- the workload of the Data Governance Office, which coordinates the drafting and approval of DSAs.

Requesting the data

If you have not already done so, ensure you have separately requested the data to be covered by the DSA. Requests for UNSW data can be made using the following links/emails:

- SiMs / UAC data from the Info Hub Data Platform online request form
- HR/PiMs data HRDReporting@unsw.edu.au

Confirming whether a data sharing approval is needed

When the Data User is from UNSW, a DSA is the typical form of written permission from the Data Custodian.

When the Data User is from outside UNSW (including system/service vendors and suppliers), the procurement contract is the main form of written permission, but an External DSA may also be required.

A DSA is needed when UNSW data is accessed or viewed by, transferred to, shared with, or used by…

Scenarios	Examples
Another UNSW Information system	E.g. Student (SiMs) data is shared with the Complaints Management System
Another UNSW Business Unit	E.g. SiMs data is shared with Divisions/Faculties for bespoke databases, PBI etc

A procurement contract (provided and facilitated by UNSW Procurement) and/or External DSA is needed when UNSW data is accessed or viewed by, transferred to, shared with, or used by…

Scenarios	Examples
An external information system, platform, service, SaaS (including new Enterprise systems)	E.g. Staff (PiMs) data is shared with FCM Travel's Pre-Travel Approval System
An external party	E.g. SiMs data is shared with consultants for course reviews, ranking bodies, and accreditation organisations

And in some cases, a DSA may not be needed…

Other scenarios	Is a DSA needed?
Researcher uses research data in PBI dashboard	**YES –** If the dataset includes any data from UNSW enterprise data systems e.g. PiMs or SiMs **NO –** If the researcher (or their research team has custodianship/has generated the data) **NOTE -** Researchers should only use personal information (PI) if they have Ethics approval
Staff member wants to create automated approval linking supervisor data in workflow	**YES –** If there is a data feed from PiMs **NO –** If the person whose PI is involved has input the data themselves into a form - **however** there should be a Privacy Notice on the form seeking consent for the PI to be used and a description of the use
Staff member 'self-serves' data from SiMs or PiMs for use in another database or PBI	**YES**
Development of chatbots or databases that use PiMs, SiMs (even if directly input) or other UNSW enterprise data	**YES**

Gathering the information to complete the request

The Data Governance Office requires certain information to approve your request for a data sharing approval. This information includes as follows:

- UNSW data: a table listing every individual UNSW data field to be covered by the data sharing approval
- purpose: how the UNSW data will be used
- transfer: how the UNSW data will be transferred from the source UNSW information system to you or another information system
- storage: where the UNSW data will be stored once it has been transferred to/ shared with you for use
- access:
- who will have access to the UNSW data (including being able to view, download, share, or use the UNSW data)
- what security measures will be used to restrict access
- how access approval is granted and how often access is reviewed

- reports:
    - will any reports be produced from the UNSW data if yes, will the reports be aggregated or contain personal information
    - where will the reports be stored
    - who will receive the reports
- personal information: does the UNSW data contain any personal information (typically any information that can be used to identify a person)
- contract / procurement agreement: if an external or new enterprise information system, platform, service, SaaS will view, share, access or use the UNSW data
- cyber approval: if relevant, has Cyber approval been sought

Requesting a data sharing approval

Once the information set out above has been identified, a data sharing request form should be completed and submitted to the Data Governance Office.

Once your request has been submitted, the following steps will occur:

- **Information requested:** you will receive an email requesting the additional information listed above
- **Data Sharing Approval drafted**: once you have provided the additional information, the Data Governance Office will draft your Data Sharing Approval
- **Privacy review**: if the data includes personal information, Privacy will review any contract / procurement agreement and the DSA
- **Cyber review**: if relevant, a completed CSRA Stage 3 may be required before the DSA can be approved
- **Approval meeting**: Once the DSA is complete, an approval meeting will be held with the Data Custodian and other relevant stakeholders to approve the DSA.

External data sharing approvals

Where data is to be shared with a system external to the University, the data user is responsible for consulting with UNSW Privacy Officer to determine whether an external data sharing approval is required. If the UNSW University Privacy Officer determines that the procurement agreement with external System Owner adequately binds the external data user regarding its handling of the data, then an approval may not be required.

If the UNSW Privacy Officer determines that an external data sharing approval is required, the data user is required to submit a request form.

To complete the data sharing approval request, the data user must work with the System Owner of the source system to produce a detailed table of required data to the Data Governance Office.

Upon receipt of the data user's request, the Data Governance Office will (i) identify and request any additional information required, such as a Procurement Agreement, system classification or cyber assessment of the destination system; draft the external data sharing approval;

provide the draft to the data user for review and incorporation of the data field table; and liaise with the data user to finalise the draft.

If the Data Governance Office request that a cyber security review of the destination system be conducted, UNSW IT/Cyber must:

- provide the data user/ Information System Owner with the vendor risk assessment questionnaire to be completed by the System Owner;
- review the completed vendor risk assessment report as a result of the completed questionnaire once it has been returned; and
- advise the Data Governance Office whether the destination system meets UNSW security requirements, along with required mitigation if necessary.

If the destination system is found by the cyber security team to have vulnerabilities that could result in material risk, the System Owner is required to provide a plan to resolve the vulnerabilities to the satisfaction of Cyber and/or Chief Data Officer and the Data Custodian.

Where the System Owner is unwilling or unable to propose such a mitigation plan, the Data Custodian may choose to withhold approval for the external data sharing approval. Consideration should be given to whether acceptance of the mitigation plan, or withheld approval for the agreement, results in a residual risk that should be reported to the Director of Risk.

Following completion of the draft data sharing approval, the Data Governance Office will convene a first pass meeting with the data user, UNSW Privacy Officer (if the data includes PII), relevant Information System Owner/s and any other relevant employees from UNSW IT, Cyber or UPP to clarify/confirm the following details:

- who has permission to access/use the data and how that permission is controlled
- how the data will be accessed/transferred, used, stored and disposed of when no longer required
- if the data includes personal information and how that data will be managed and protected.

The Data Governance Office will then incorporate any updates to the draft external data sharing approval arising from the first pass meeting, convene a second pass meeting with the data custodian and data user and any other relevant stakeholders to review the proposed approval and address any concerns arising.

At the conclusion of the second meeting the Data Governance Office will submit the draft approval to the external data user/ System Owner for review and if necessary, convene a meeting of the external data user/ System Owner with the Data Governance Office and any relevant stakeholders to reach agreement on the draft.

The Data Governance Office will then submit the external data sharing and information approval to the Data Custodian for signature, and then to all other parties for their signature and provide a PDF of the signed approval to the data user, external data user and the Data Custodian (if required) and file the PDF in the repository.

Data transmission[18]

Before transmission of digital information to non-OECD member countries (including for processing or storage) occurs, the proposed transmission must be referred to the Chief Information Security Officer (CISO) or their delegate for additional control requirements. It is necessary to engage with the CISO and the Cyber Security Team for guidance based on the specific requirements and circumstances.

Requesting Commonwealth data

UNSW is now accredited to lodge data requests through Dataplace, an online portal for accredited Data Users to request Australian Government data not already available through data.gov.au.

The *Data Availability and Transparency Act 2022* (Cth) established the DATA Scheme to provide a consistent and efficient way for Australian Government data to be requested and a secure way for the data to be shared. Publicly available data **does not** require a Dataplace request.

This means Australian Government Data Custodians may require UNSW researchers to request data through Dataplace rather than directly from the government agency.

Accreditation as a Data User can only be obtained by the University at the organisational level.

How to request Commonwealth data

UNSW researchers can lodge a Dataplace request with the assistance of the UNSW Dataplace Data Coordinator. To initiate a request UNSW researchers must:

(i) confirm the data isn't already publicly available from data.gov.au.
(ii) if the data isn't publicly available, register your data request with the UNSW Data Coordinator by completing this short Form.

The Data Coordinator will contact you to finalise and submit your data request.

[18] See clauses 5.7 – 5.11 of the Data Governance and Management Procedure in the Information Governance Policy.

Research data sharing approvals[19]

Why do you need a Research Data Sharing approval?

Sharing of unpublished research data (internally or externally) should always be documented with ethics and/or data sharing approval. Research data sharing approval must cover research data and materials ownership, sharing, storage, accessibility, retention, and disposal.

UNSW is committed to maintaining the security, integrity and appropriate management of its data. To fulfil this commitment, UNSW limits UNSW data access to authorised users, only uses UNSW data for an agreed purpose, does not disclose UNSW data to third parties without prior approval, and securely stores and responsibly disposes of all UNSW data.

Research Data Sharing Agreements (DSAs) are used to record the agreed basis upon which UNSW will share research data with, or from, an external third party.

To create a Research DSA:

1. Download the Research DSA template
2. Follow the guidance in the template to identify and agree the required details with the external third party
3. Consult RDM@unsw.edu.au with any queries regarding research data storage

Contact datagov@unsw.edu.au with any queries regarding completion of the template.

Once the finalised Research DSA has been signed by both parties, a copy must be sent to datagov@unsw.edu.au.

Sharing and transmission of sensitive research data

Researchers will often be required to share research data with other collaborators or organisations. If research data is sensitive, researchers will need to pay attention to how it is shared, who it is shared with, and the length of access.

ANDS (now part of the Australian Research Data Commons) has a guide on sharing sensitive data, focused on publishing. For tips and advice on sharing and transmitting research data see Data Sensitivity & Classification (sharepoint.com)

Secure platforms for storing and with working with sensitive data

Platforms such as **SURE**, **ERICA**, and **SeRP** are designed for storing and working with secure data. Some providers may require the use of one of these platforms to access to their data, however technical options can only go so far to protect data. Researchers should consider adding extra restrictions such as legal agreements before the start of an activity or project.

Data Use Conditions[20]

In addition to considering the Intellectual Property (IP) Policy, Research Authorship, Publication and Dissemination Policy, UNSW Open Access Policy, researchers should consult guidance on applying the appropriate protections and controls to their data for use. Protecting your data is crucial to ensure research data remains secure, while being as open as possible, to ensure it is utilised to the fullest extent.

The UNSW Library offers support for researchers to understand and apply copyright, open access principles, and for publishing and sharing research. Researchers must abide by conditions restricting use of research data.

Re-use of existing data

Researchers using existing research data to inform their research project or activity must have permission and meet the conditions for re-use, including the retention and disposal requirements, and document this in the RDMP.

International import and export of research data[21]

Research data and materials are subject to export controls, as regulated by the *Customs Act 1901* (Cth), *Defence Trade Control Act 2012* (Cth) and applicable sanctions in force at the time of export.

Before exporting or importing research data and materials involving 'controlled' goods, technology, software and/or activities as defined by the Defence and Strategic Goods List (DSGL) 2021for research projects, UNSW researchers must first check domestic and international import/export requirements and obtain relevant permits.

Researchers exporting research goods, data or technology must comply with the Research Export Controls Procedure. For guidance on obtaining relevant permits, researchers should contact the Research Ethics & Compliance Support Office (exportcontrols@unsw.edu.au).

Researchers travelling internationally with research data and materials must consider before travelling who is allowed to access secure data and materials under local laws.
Researchers must also consider domestic and international privacy requirements when importing or exporting human research data or materials, if unsure about the applicable privacy requirements, researchers should contact the UNSW Legal & Compliance at privacy@unsw.edu.au who will determine whether a Privacy Impact Assessment is required.

[19] In the Data Governance and Management Procedure of the Information Governance Policy, see the callout box under clause 5.6 entitled "Research Data".
[20] In the Data Governance and Management Procedure of the Information Governance Policy, see the callout box under clause 5.17 entitled "Research Data".
[21] See clause 5.11 of the Data Governance and Management Procedure of the Information Governance Policy.

Researchers must ensure that research data and information is packaged and labelled in accordance with (Australian Customs requirements) to expedite the clearance of such packages through the Australian Quarantine Inspection Service (AQIS) and release by Australian Customs.

Researchers exporting research data and materials to countries impacted by sanctions implemented by the Australian Government must obtain advice to confirm if the export is permitted or otherwise requires a permit from the Department of Foreign Affairs and Trade.

List of Data Executives, Data Custodians & Data Stewards

The list of Data Executives is available here. The Data Executives are those listed as part of the University Leadership Team.

The list of Data Custodians is available here.

The list of Data Stewards is available here.

Research Offboarding and exit planning

Researchers leaving UNSW with a role in a research activity or project, who will no longer have a zID, must share data storage locations, data management information, access permissions and transfer custodianship to the researcher replacing their role before leaving UNSW to ensure there is continuous custodianship of research data.

During the offboarding process, a reminder will prompt researchers to ensure they have fulfilled their obligations before they leave, with the supervisor confirmation.

Misconduct & Complaints[22]

Data Custodians and/or researchers must report potential misconduct or breaches of the UNSW Code of Conduct and Values; and/or the Australian Code for the Responsible Conduct of Research 2018, and/or any UNSW policies; and/or any legislative requirements to the Research Integrity Officer for their faculty in the first instance.

See the Complaints Management and Investigations Policy and Procedure for further information.

[22] In the Data Governance and Management Procedure of the Information Governance Policy, see the callout box under clause 5.17 entitled "Research Data".

Section 2: Records and Information Management

A record is any document you make or receive as part of your work that provides evidence of action. Records can be in any format.

The University owns all records created and received by its employees. These records provide evidence of what was done or decided and together, they form a vital University asset.

Capturing records[23]The capture of a record at its point of creation and in its original format saves resources, increases evidentiary value and aligns recordkeeping to improved business outcomes.

Recordkeeping should be an inherent, integrated and allocated part of everyday business.

Systems of Record

All records must be captured to a University System of Record. These are business systems that have been evaluated to ensure the requirements of a record are met, such as their fixed evidentiary nature, retrievability, security controls and lifecycle management.

Records and Information Management (RIM) Stewards are responsible for the capture of all records to a System of Record.

RAMS (Records & Archives Management System)

RAMS is the University's enterprise recordkeeping system accessible to all University staff for the secure capture of records not directly captured by alternative Systems of Record.

For more information on how to capture a record to RAMS, view the RAMS tutorial instructional video, visit the RAMS SharePoint page or contact the Records & Archives Office.

Unlisted systems of record

RIM Stewards are responsible for completing the appropriate System of Record Assessment if:

- a business system being used to capture a record is not listed as a current UNSW System of Record, or
- a new business system intended to capture and store University records is being procured or developed, or
- a business system is being decommissioned.

[23] See clauses 2.1 – 2.6 of the Records and Information Management Procedure in the Information Governance Policy.

RIM Stewards should contact the Records & Archives Office for assistance with completing the assessment.

What does not constitute a UNSW System of Record?

- email accounts
- network drives
- cloud-based network drive providers (e.g. Dropbox, Google Drive)
- collaborative tools (e.g. MS Teams, WhatsApp)

Records stored in these systems must be captured to RAMS or an alternative System of Record.

Titling records

The University has an approved Guideline for titling. You can access it here.

It is recommended to title records consistently across media to allow for consistent identification, capture and retrieval of information. The Guideline provides best practice advice on how to do this.

Accessing records[24]

Staff can:

- search for records through the RAMS interface
- request a search be conducted by Records & Archives staff
- access as well as request delivery of hardcopy UNSW records (subject to Security Level and Caveat restrictions)
- all staff members receive automated access to relevant Security Levels and Caveats based on their position. Any staff member wishing to confirm their access may contact the Records & Archives Office for further information
- conduct a search of the University Archives.

RAMS Access Control

When capturing a record to RAMS, RIM Stewards are responsible for applying access controls based on UNSW data classifications.

RIM Stewards should refer to the table below to:

- map the University's data classifications against the required controls in RAMS,
- determine whether transmission of this information by email is appropriate, and
- determine how frequently the security controls of this information should be reviewed.

[24] See clauses 2.2, 2.8, 3.3 and 6.2 of the Records and Information Management Procedure in the Information Governance Policy.

RAMS Access Controls				
	HIGHLY SENSITIVE	**SENSITIVE**	**RESTRICTED**	**UNOFFICIAL/PUBLIC**
RAMS Access Control Requirement	Mandatory restriction. Access control must be applied to restrict only those positions and/or business units that require access to this information.	Mandatory restriction. Access control must be applied to restrict all Units/Departments that require access to this information.	Optional, required for business purposes only.	Optional, required for business purposes only.
Access controls	View document: <Special Access Group or individual positions View metadata: <Special Access Group or individual positions>	View document <Division or subgroup> View metadata <Division or subgroup>	View document <Division or subgroup> View metadata <Division or subgroup>	View document: <Unrestricted> View metadata: <Unrestricted>
Review period	Every 6 months	Every 1 year	Every 2 years	Not required

Retaining records[25]

Records must, irrespective of format, be stored in an appropriate, secure location.

The University maintains a permanent collection of archives on-site. Records that are identified as being archival are required to be retained permanently by the University. Further information is available here.

Offsite storage of hardcopy records

RIM Custodians are responsible for ensuring the Records & Archives Office arranges the offsite storage of hardcopy records with an approved storage provider.

Hardcopy records must be appraised before being transferred, which means identifying the minimum legal periods for records retention using the NSW Disposal Authorities listed on the

[25] See clauses 2.6, 3.6, 3.7, 4.1 and 4.2 of the Records and Information Management Procedure in the Information Governance Policy.

Records & Archives website. Although appraisal is usually undertaken by the Records & Archives Office, RIM Custodians can choose to appraise records themselves by following the appropriate guidance.

Conversion of hardcopy records to digital records

An alternative to storing hardcopy records offsite is to have them scanned and captured to a UNSW System of Record such as RAMS.

RIM Custodians should contact the Records & Archives Office to arrange record digitisation, and ensure the recommended minimum technical specifications for scanning are addressed.

Note: Conversion of records only impacts their format; it has no bearing on the minimum legal period for which they must be retained.

Research data retention[26]

Retention of research data and supporting research records

Researchers have an obligation to retain clear, accurate, secure and complete records of all research data, research materials, and supporting research records.

In addition to the UNSW recommendations, researchers, in conjunction with Data Custodians, must consider state and federal legislations, journal publisher requirements, and funding bodies when nominating a retention period for their research data.

Records and Information Management and the Research Data Management Team have developed a Guide to Retention Periods for Research Data and Records which supports researchers to understand and meet their legal obligations:

Retention Period for Research Data

Category	Examples Data & Datasets	Retention Period
A	• involving community or heritage significance • relating to genetic research, including gene therapy • containing controversial issues or of high public interest, or has influence in the research domain • costly or impossible to reproduce or substitute if the primary data is not available • relating to the use of an innovative technique for the first time	**Permanently**
B	• from clinical trials • involving research with potential long term effects on humans • not covered by Category A	**Minimum 15 Years** after completion of research or until patient would be 25 years old, whichever is the longer
C	General research data not covered by the Category A and B	**Minimum 5 Years** after completion or publication of research, whichever is the longer.
D	• for assessment purposes only • not covered by Category A, B and C	**Minimum 12 Months**

Please note that research data and its supporting records should never be destroyed without consulting the complete process. For more information, go to https://www.recordkeeping.unsw.edu.au/recordkeeping/destroying-records or contact rdm@unsw.edu.au.

The Guide to Retention Periods for Research Data and Records also outlines the retention periods for supporting research records related to:

[26] In the Records and Information Management Procedure of the Information Governance Policy, see the callout box under clause 4.2 entitled "Research Data".

- Ethics Committee Processes
- Intellectual Property Rights
- Research Reporting
- Project Administration

For more in-depth information about these retention requirements in relation to research, refer to the complete Guide.

If different types of data have different retention periods, researchers should select the longest retention period (e.g., if once type of data requires 5 years and another requires 15 years, select 15 years)
If you have specific retention periods for certain data sets (e.g., grant funding or ethics requirements), you can describe them in the additional details field.

Note: The data retention date does NOT mean your data will disappear without consultation at the time recorded.

UNSW Supported platforms have set retention periods in the Guide above, but if a researcher uses external platforms they must ensure that research data is archived appropriately at the end of a project, and disposed of securely and at the appropriate time.

Research records are subject to a 'closed to public access' (CPA) direction to close the records for 30 years. The UNSW Access Directions lists UNSW records currently subject to a CPA direction.

Researchers who re-use existing research data to derive new research data must nominate a retention period for the new research data. However, if a new research data set is derived which can be reproduced using existing data, researchers should avoid unnecessary duplication and retention of existing data and instead retain how the derived data set can be reproduced.

Publication of Metadata about Research on UNSWorks

Data can be made more "reuseable" when it is properly licensed. Attaching a license can also help protect your work. Unless otherwise stated, materials deposited in the UNSW Open Access institutional repository, UNSWorks, are protected by the Copyright Act 1968 and are licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives Licence (CC BY-NC-ND).

Your Outreach Librarian would be able to advise on licensing matters.

The library's UNSWorks institutional repository webpage also provides details around the different kinds of licenses available when depositing materials into the UNSW Open Access institutional repository, UNSWorks.

Destroying records[27]

Who can destroy a record?

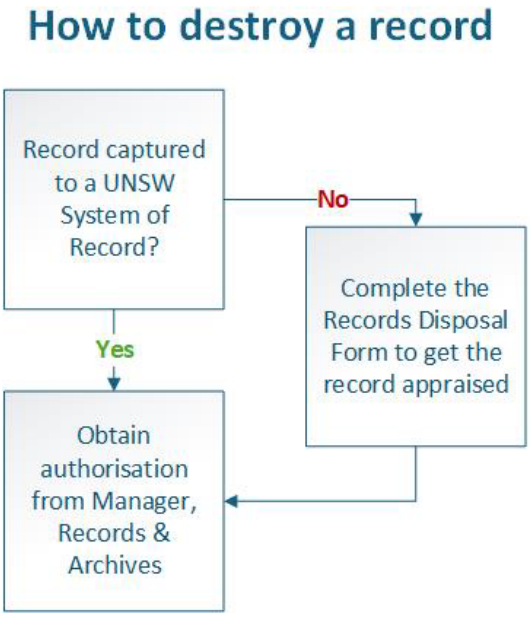
RIM Stewards must receive the authorisation of the Manager, Records & Archives before records at UNSW can be destroyed.

Before receiving this authorisation, RIM Stewards should complete the Records Disposal Form for records that need appraisal. This form provides the Records & Archives Office with the necessary information to undertake appraisal.

Records captured to a UNSW System of Record have already undergone a process of appraisal and do not require further action.

Appraisal decisions are made in accordance with the requirements of the State Records Act 1998 (NSW) adhering to the conditions defined by the General Retention and Disposal Authorities (GDAs) issued by the State Records Authority NSW. These GDAs define the minimum legal period for which records must be retained.

The process of appraisal is also important for the purpose of identifying records of an enduring nature that may be required to be retained permanently as archives. Information on what constitutes a State or a University Archive, and on the process for the donation of Private Papers to the University is described here.



[27] See clauses 5.1 – 5.4 of the Records and Information Management Procedure in the Information Governance Policy.

RIM Stewards should complete the System Decommissioning Assessment if a business system listed as a current UNSW System of Record is planned to be retired.

When not to destroy a record

Records may not be destroyed when subject to:

- current or reasonably anticipated legal proceedings where the records may be required as evidence.
- an application for access under the *Government Information (Public Access) Act 2009* (NSW), the *Health Records and Information Privacy Act 2002* (NSW) or the *Privacy and Personal Information Protection Act 1998* (NSW)
- a government policy or directive not to be destroyed.

Normal Administrative Practice (NAP)

NAP provides for the destruction of low-value records of no continuing value. . These records include:

- **Drafts** - Any version prior to the final version of a record that does not document significant decisions, discussions, reasons and actions or any significant information that is not contained in the final captured version of the record.
- **Working papers** - Papers, background notes and reference materials that are used to prepare or complete other record that do not document significant decisions, discussions, reasons and actions or contain significant information that is not contained in the final version of the record
- **Duplicates** - Copies of records that have already been captured within a recordkeeping system and that are generally held only for reference purposes.
- **Backups** - Backups are facilitative records only. The NSW State Records Authority specifically advises against backups being relied upon as official records of business. They should be destroyed when no longer required under the provisions of Normal Administrative Practice (NAP) with no additional steps required.
- **Solicited and Unsolicited advertising material** – This includes junk mail and spam.

Note: Any records that hold continuing value to the University, being those that have administrative, business, fiscal, legal, evidential or historic value should not be destroyed using NAP.

Research data disposal[28]

Determining when to dispose of research records

There is a significant cost to the University in storing records for periods longer than those for which the University is legally obliged to retain the records. Records should, therefore, be destroyed once their retention period have expired and they are no longer required for their original purpose.

Records which are required for known, or reasonably anticipated, litigation, inquiries or investigations, or records that may be relevant to allegations of research misconduct must not be destroyed or otherwise disposed of until the litigation or investigation has been concluded. They should not be retained 'just in case' litigation or inquiries may arise at some time in the future. View Destroying Records for further information on the processes at UNSW.

Disposal of Normal Administrative Practice (NAP) research data

Researchers should dispose of certain types of research data during the research data life cycle using NAP, in accordance with State Records Regulation 2024 - NSW Legislation, Schedule 2 Guidelines on what constitutes normal administrative practice—the Act, s 22(3).

For example, research data can be disposed of via NAP if it is:

Category	Description	Examples
Transitory or Ephemeral data	Data needed only for a short period, such as preliminary results or temporary datasets, not required to justify research output.	1. Intermediate files or temporary datasets generated during processing that are necessary for the final output but can be regenerated using the code and initial data. 2. Failed scans and other data generated from instruments that is not needed to justify research outputs
Duplicate	Non-master copies of research data	1. Copies of data on High Performance Computing Scratch storage 2. Copies of data on local computer disks with a master copy located elsewhere (e.g. OneDrive) 3. Copies of 3rd-party public datasets, where the dataset is available in a long-term repository 4. Copies of UNSW Datasets provided to collaborators, where not required by the external party

Drafts not intended for further use	Draft documents without significant changes or annotations, not required for justification of research output	1. Drafts of research papers without significant differences to final copies
Unofficial information	Unsolicited emails or personal notes unrelated to research activities	1. Personal communications and meeting invites 2. Unsolicited emails from 3rd parties

Retention and Disposal of Research Data containing Personal Information

In consideration of privacy obligations under the *Privacy and Personal Information Protection Act* 1998 (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) UNSW stores and retains research data containing personal information (PI) (classified as sensitive or highly sensitive) only for the minimum duration it is legally and operationally required, and access is strictly limited.

Once the minimum retention period has been met the researcher, in conjunction with the Data Custodian, must review the retention period and dispose of research data containing PI. If research data is nominated or appraised for permanent retention on the basis of '*regulatory or community significance*', per General Retention and Disposal Authority (GA0047) then personal information may require additional protections, such as de-identification or masking.

For further information, please see Personal information | Records & Archives - UNSW Sydney or contact privacy@unsw.edu.au and records@unsw.edu.au

Metadata for records and information management[29]

Metadata assists in locating resources and provides context to understand the value of information.

Minimum metadata set

State Records NSW indicates that for authoritative records and information, the minimum metadata required includes:

- a description of the content of records and information
- the structure of records and information
- the business context in which the records and information were created or received and used
- relationships with other records, information and metadata
- business actions and events

[28] Ibid.
[29] See clauses 3.1 and 3.2 of the Records and Information Management Procedure in the Information Governance Policy.

- information that may be needed to retrieve and present records and information

This minimum metadata set can be applied to UNSW Systems of Record (e.g. RAMS), individual records or groupings of records.

Applying the minimum metadata set to UNSW records

RIM Stewards can map the minimum metadata set against relevant metadata fields from the AS/NZS 5478:2015 *Recordkeeping Metadata Property Reference Set (RMPRS)*. The RMPRS provides a reference set of recordkeeping metadata that UNSW can use.

For guidance on how to apply the minimum metadata requirements, contact the Records & Archives Office.

Additional metadata requirements

RIM Stewards may need to capture metadata beyond the minimum requirements, depending on the UNSW System of Record.

For example, when capturing new records in RAMS, RIM Stewards are prompted to complete a specific set of relevant metadata fields. These include:

- mandatory metadata fields - **Title**, **Container** and **Date Created**.
- optional metadata fields - **Author**, **Addressee**, **Security**, **Record Number** and **Document Category**.

For records already stored in RAMS, these metadata fields can be edited. The RAMS Quick Reference Guide contains further information on metadata for records in RAMS.

For guidance on capturing metadata for records in other UNSW Systems of Record, contact the Records & Archives Office.

RIM Stewards should ensure that, for externally acquired data, the metadata refers to contractual agreements and the effective dates and times of the data. This will assist in:

- compliance with licensing terms,
- understanding the validity period, and
- managing data usage according to contractual obligations.

RIM Stewards should further ensure that:

- access to metadata records is restricted when necessary to meet accountability, legislative and business requirements
- deletion of metadata records does not take place unless part of authorised disposal activity.

Section 3: Privacy

Privacy Impact Assessment[30]

A Privacy Impact Assessment (PIA) must be conducted for any project (other than a research project or activity) that is likely to involve a "high risk" to people's personal information, including:

- large-scale use or disclosure of sensitive personal or health information
- systematic and extensive profiling of individuals
- public monitoring (e.g. CCTV)
- use of AI to support decision making
- any use of biometric or genetic data
- "invisible processing" where personal information has not been collected directly from the individuals concerned
- where the use is of such a nature that a data breach could jeopardise the health or safety of individuals.

Determining whether a PIA is required

The University Privacy Officer will conduct a threshold assessment to determine whether a PIA is required by considering the following:

- the kinds of data or information being collected/accessed, and specifically whether the information is personal/sensitive information
- where personal information/data is flowing to or from
- the purpose and use of the information
- the nature of consent required (e.g., consent to data collection and use/purpose is covered within the existing PMP, student privacy statement, etc) or express consent needs to be obtained
- if any new personal information is being created as a result of the project
- information management
- storage/security
- disposal
- the data sharing approval to ascertain the types of data and/or information being used/collected etc
- the contract and terms of use where there is a third-party vendor
- any communications to stakeholders/users where their personal information is affected/used/collected etc.

If the University Privacy Officer determines that the personal information and/or health information is involved, and there is a "high risk" to individuals, the Privacy Officer will request that a PIA be conducted using the PIA template.

[30] See clauses 2.1 – 2.4 of the Privacy Procedure in the Information Governance Policy.

On completion of the PIA, the University Privacy Officer will assess and map the flow of personal and/or health information. The map will detail what information will be collected, used and disclosed, as well as how it will be stored and protected. The mapping will describe:

- who will collect what information, and from whom
- how the information will be collected, and for what purpose
- how the information will be used or processed
- how the information will be stored and kept secure
- the processes for ensuring information quality
- whether the information will be disclosed to another agency or organisation, to whom and for what purpose
- if the information is to be disclosed to and used by secondary users, assess how those secondary users will protect that information and under what conditions they are permitted to share the information with others
- whether personal information will be transferred to another organisation in another jurisdiction either in Australia or overseas
- whether individuals will be able to access and correct their personal information
- how long the information will be retained and when and how the information will be disposed of.

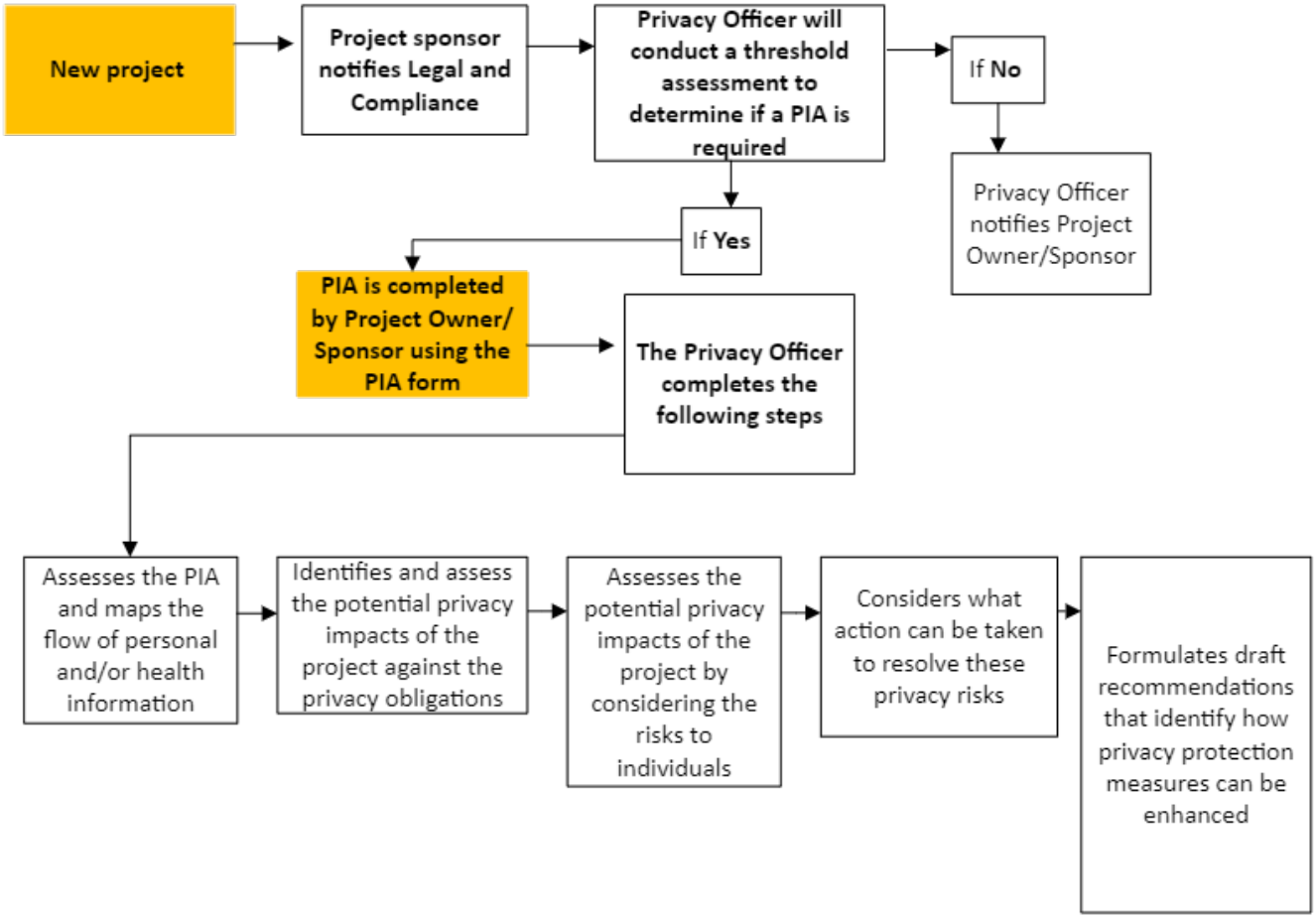
Once the mapping has been completed, the University Privacy Officer will identify and assess the potential privacy impacts by considering:

- the PPIP Act and HRIP Act and regulations
- any applicable Privacy Codes of Practice and Public Interest Directions
- where applicable, Commonwealth privacy legislation
- other legislation that applies to UNSW relating to the collection and use of personal and health information.

In addition, the University Privacy Officer will assess the potential privacy impacts by considering the risks to individuals, such as the potential re-identification of pseudonymised data and/or information, identity theft or fraud, reputational damage, loss of confidentiality or financial loss.

Once this assessment has been completed, the University Privacy Officer will consider what action can be taken to resolve or adequately mitigate these privacy risks and formulate draft recommendations that identify how privacy protection measures can be implemented or enhanced and the ways in which negative privacy impacts or risks can be avoided or reduced.

The following flowchart summarises the steps for requesting and completing a PIA.



Right to Information[31]

The options and procedures for seeking information are outlined on the UNSW Legal & Compliance section of the UNSW website under privacy and access to information.

The UNSW Privacy Management Plan additionally summarises the processes for seeking access to personal information.

Members of the public, students or staff and affiliates may request access to their personal information by contacting the relevant business unit of the University that holds the information or make the request to the University Privacy Officer.

Such requests for personal information can be made under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). Health information can be sought under the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). If the individual does not receive access to the information requested or experiences delay in receiving a response to a request under the PPIP Act or HRIP Act, the individual can seek a privacy internal review with the University Privacy Officer.

Members of the public and students or staff may also apply under the *Government Information (Public Access) Act 2009* (NSW) (GIPA Act) for access to any information held by the University, including information about themselves.

[31] See clauses 3.1 – 3.4 of the Privacy Procedure in the Information Governance Policy.

Requests can be made informally or formally under the GIPA Act. Informal requests can be made by contacting the Right to Information Officer on the following details.

Right to Information Officer
Phone: (02) 9348 1198
Email: gipaa@unsw.edu.au

Information about the informal requests for information is available at Frequently asked questions for citizens: Informal release of information (nsw.gov.au).

How to make a formal access application under the GIPA Act

To make a valid formal access request under the GIPA Act, the application must:

- be in writing
- state that it is made under the GIPA Act
- state the name of the applicant
- state a postal or email address as the address for correspondence in connection with the application
- provide enough details to help the University identify the information you want
- be accompanied by the statutory application fee of $30.

Formal access applications should be submitted to the Right to Information Officer at UNSW using this form.

Information regarding the cost and duration of a formal access application is available on the University's webpage on access to information.

Applicants who have been refused access to the information requested or are dissatisfied with the decision made by UNSW in response to their formal access application can seek:

- an internal review of the decision with UNSW; or
- a review by the Information Commissioner; or
- a review by the NSW Civil and Administrative Tribunal (NCAT).

Information regarding reviews is set out on the University's webpage on Access to Information.

Protecting the privacy of individuals

The Information Protection Principles (IPPs) in the PPIP Act and the Health Privacy Principles (HPPs) in the HRIP Act are designed to ensure personal and health information respectively that is held by the University is not modified, used or accessed by unauthorised people. The IPPs and HPPs regulate the handling of personal and health information, and cover its collection, storage, use, disclosure and disposal.

Examples of conduct by the University that would be contrary to the IPPs and HPPs include:

- collecting personal or health information that does not directly relate to or is not necessary for a UNSW activity/function
- collecting personal or health information from someone other than the person concerned (unless otherwise authorised)
- collecting personal or health information from someone without informing them why and for who it is being collected
- storing personal or health information for longer than necessary and without protecting it from unauthorised access, use, modification or disclosure
- placing excessive time or monetary restrictions on someone's ability to access their personal and health information held by the University
- restricting someone's ability to update, correct or amend their personal or health information where necessary
- using personal or health information before checking its relevance, completeness and accuracy
- using personal or health information for a different purpose than when it was collected (unless consent is granted, or someone's personal health/safety is at risk)
- disclosing personal or health information without someone's consent
- disclosing sensitive personal information without someone's consent (examples of sensitive personal information include ethnic or racial origin, political opinions and religious beliefs).

An individual who believes that the conduct of the University in handling their personal information is contrary to the IPPs or HPPs is entitled to a review of that conduct.

Privacy complaints[32]

The options for lodging a privacy complaint are set out in the UNSW Privacy Management Plan.

Whilst complaints are encouraged to be resolved informally, an individual has the right to seek review either:

(1) under the UNSW Complaints Handling Policy and Procedure OR
(2) through an internal review under the PPIP Act.

If an individual is dissatisfied with (1), they can pursue (2).

The Legal & Compliance section of the UNSW website details the option to raise a privacy complaint in the form of a privacy internal review with UNSW under section 53 of the PPIP Act.

Privacy internal review

[32] See clauses 4.1 and 4.2 of the Privacy Procedure in the Information Governance Policy.

A request for a privacy internal review with UNSW can be made where it is alleged that the University has:

- breached any of the IPPs or HPPs; or
- breached any code made under the PIPP Act applying to the University; or
- disclosed personal information kept in a public register of the University.

An application for a privacy internal review must:

- be in writing
- be addressed to the University
- specify an address in Australia to which the applicant is to be notified after the completion of the review, and
- be lodged with the University Privacy Officer within six months form the time the applicant first became aware of the conduct to be the subject of the review.

Requests for a privacy internal review are preferred to be submitted to UNSW using this form.

A person who is not satisfied with the outcome of a privacy internal review can seek an administrative review at the NSW Civil and Administrative Tribunal (NCAT). Further information about review rights following a privacy internal review is available within the Information and Privacy Commissions factsheet Privacy complaints: Your review rights (nsw.gov.au)

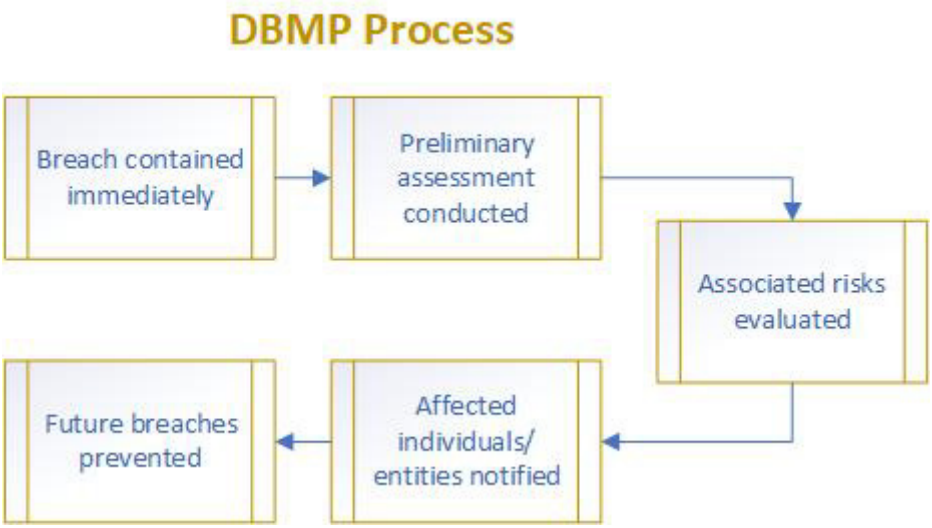
The University Privacy Officer can also be contacted regarding privacy internal review matters at privacy@unsw.edu.au.

Section 4: Data breaches

The Data Breach Management Plan[33]

As outlined in the flowchart, the lead investigator will enact the Data Breach Management Plan (DBMP) upon referral of a suspected, confirmed or eligible data breach.

The following diagram outlines the DBMP steps:



1. Immediately contain the breach and conduct a preliminary assessment

1) The lead investigator will conduct a preliminary assessment and recommend actions to contain the breach.

2) The breach will be contained by immediately making all reasonable efforts to stop the unauthorised activity; and/or recover or limit the dissemination of records disclosed without authorisation; and/or shut down a compromised system.

The following questions will be addressed by the lead investigator in their preliminary assessment:

- who is affected by the breach?
- what information does the breach involve?
- if the information contains personal information and/or health information, what types of personal information or health information does the breach involve?
- does the breach amount to a loss of personal information or health information held by UNSW likely result in unauthorised access to, or unauthorised disclosure of, the information?

[33] See clause 6.1 of the Data Breach Procedure in the Information Governance Policy.

- would a reasonable person conclude that the access or disclosure of the personal or health information will likely result in serious harm to an individual to whom the information relates?

In deciding whether the breach would be likely to result in serious harm to an individual to whom the information relates, the lead investigator will consider the following:

- the types of personal information or health information involved
- the sensitivity of the personal information or health information
- whether the personal information or health information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused
- who had access to the personal information or health information
- whether the person/s who accessed the personal information or health information may have malicious intent and whether they may be able to circumvent security measures
- the nature of the harm that has occurred or may occur.

Further information about the assessment of eligible data breaches and what is serious harm as part of the assessment of the data breach can be found in the Information and Privacy Commission (IPC) MNDB Scheme resources available at Privacy Resources for Agencies (nsw.gov.au), including the factsheet available at Guidelines on the assessment of data breaches under Part 6A of the PPIP Act (nsw.gov.au).

2. Evaluate the risks associated with the breach

The lead investigator will assess the risks associated with the breach by considering the following questions:

- what was the cause of the breach?
- what is the extent of the breach?
- is there a risk of ongoing breaches or further exposure of the information?
- is there evidence of theft?
- is this a systemic problem within UNSW or an isolated incident?
- how many people are affected by the breach?
- what other harms could result from the breach?
- have there been other breaches that could have a cumulative effect?
- how could the information be used?
- has the information been recovered?
- what steps have already been taken to mitigate the harm?
- is there a reputational risk to UNSW?
- is there a commercial or intellectual property risk for UNSW?

If there are reasonable grounds to suspect, or there is evidence to conclude, that an eligible data breach or a data breach has occurred, the lead investigator will immediately report their conclusion to the General Counsel and the DBM committee.

3. Notifications to affected individuals or entities

Where the lead investigator concludes or has reasonable grounds to suspect that the breach amounts to an eligible data breach and the General Counsel agrees with this assessment, the General Counsel will:

- immediately notify the Privacy Commissioner of the eligible data breach using the approved form published by the Privacy Commissioner, unless it is not reasonably practicable for the information to be provided; and
- as soon as reasonably practicable, notify each individual to whom the personal information the subject of the breach relates, or each affected individual or their authorised representative, in writing about the breach, unless exempt from doing so.

The notification to each individual will provide affected individuals with an accurate description of what happened, what risks may arise and what they can do to protect themselves.

The notification will specifically contain the following information:

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred
- the personal information that was the subject of the breach
- the amount of time the information was disclosed for
- actions UNSW has taken or plans to ensure the personal information is secure
- actions UNSW has taken to control or mitigate the harm done to the individual
- recommendations about the steps the individual should consider taking in response to the eligible data breach
- information about:
  - how to make a privacy-related complaint to the Privacy Commissioner
  - how to seek an internal review of UNSW's conduct
  - the contact details for UNSW or a person nominated by UNSW for the individual to contact about the breach.

If it is not reasonably practicable to directly notify any or all the individuals affected by the breach, the General Counsel will:

- arrange to have published a public notification on UNSW's website for at least 12 months detailing information about the breach, such as: the date the breach occurred, how the breach occurred, the type of breach that occurred, the amount of time the information was disclosed, actions taken or planned to ensure the personal information is secure, where to contact for assistance or information
- take reasonable steps to publicise that notification
- provide the Privacy Commissioner with information about how to access the public notification on UNSW's website.

See the Data Breach Public Register - Legal & Compliance | Planning & Assurance - UNSW Sydney.

In addition, the DBM committee, consulting with relevant officers of the University as required, will determine if it is appropriate and necessary to notify other third parties, such as:

- the Police
- insurance providers
- credit card companies and/or financial institutions
- professional or other regulatory bodies
- other internal or external parties who have not already been notified
- agencies that have a direct relationship with the information that is lost/stolen such as State Records NSW or Museums of History NSW
- funding or partner organisations such as the National Health and Medical Research Council (NHMRC).

4. Notification to employee that reported the breach

Where appropriate, the Chair of the DBM committee informs the employee who reported the breach about the results and helps them respond to any information requests about the breach from stakeholders or other third parties.

5. Prevention of future breaches

Once immediate steps have been taken to mitigate the risks associated with a breach, and relevant notifications have been made, the lead investigator will:

- investigate the cause of the breach
- conduct a post-breach review and evaluation on the root cause of the breach
- in consultation with the General Counsel, identify if there is a risk of legal proceedings against the University as a result of the breach (e.g. class action by affected individuals) and will provide a report to the DBM committee.

The Chair of the Committee will:

- on behalf of the DBM committee, provide a brief to the UNSW Safety & Risk Committee of Council on the outcome of the post-breach review and relevant recommendations
- publish information about the data breach, the steps UNSW took to mitigate the harm done by the breach and the actions to prevent future breaches in UNSW's internal data breach incident register.

Section 5: Digital communication platforms/technologies

Storage of digital information[34]

At UNSW, users can store digital information inMicrosoft 365 apps such as Microsoft OneDrive, SharePoint and Microsoft Teams. Users are discouraged to store digital information in local storage (e.g. USB, hard drives).

Staff can manage shared network drives and folders using the File System Access Management (FSAM) tool (shared network drive).

The table below highlights the benefits using Microsoft 365 and shared network drives over local storage.

Feature	MS OneDrive & Teams	Local Storage (e.g. USB, Hard Drives)	Shared Network Drive (FSAM)
Data Classification	HIGHLY SENSITIVE SENSITIVE RESTRICTED UNOFFICIAL PUBLIC	UNOFFICIAL PUBLIC	RESTRICTED UNOFFICIAL PUBLIC
Stored in Australia	✓	possibly	✓
Backup & Disaster Recovery	✓	✗	✓
Syncing with Local Copy	✓	n/a	n/a
External Collaborator Access	✓	✗	✗
Storage Limit	Starting at 5 TB	possibly	Unlimited
Version Control	✓	✗	✓
Recovery from Deletion	60 Days	✗	10 days
Post-Project Data Retention	> 7 years	possibly	> 7 years

Visit Storing and sharing files for more detailed instructions on using each aforementioned system.

Responsible identity and access management[35]

[34] In the Data Governance and Management Procedure of the Information Governance Policy, see clauses 3.1 and 3.4 - 3.6; In the Records and Information Management Procedure of the Information Governance Policy, see clauses 3.3 – 3.5.

[35] See clauses 11.1 – 11.5 of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.

Users of UNSW information resources and digital communication platforms/technologies can visit the Secure account access page for detailed guidance on how to approach identity and access management responsibly. The page outlines the services provided by the UNSW Cyber Security team.

Users should ensure all relevant services are set up correctly so that UNSW information resources are protected when using digital communication platforms and technologies.

The services are as follows:

- zID & password - UNSW staff and students can use the UNSW Identity Manager self-service portal to manage their zID password. UNSW IT's zID and password page contains guidance on changing passwords, unlocking accounts, accessing staff forms for account access, and FAQs
- Multi-Factor Authentication (MFA) - MFA is a requirement at UNSW for everyone with a current zID account. This includes all students and staff (including casuals and affiliates). Visit Multi Factor Authentication (MFA) for guidance on all aspects of MFA, including how to set it up and viable alternatives
- Single Sign-On (SSO) - SSO is a session and user authentication service that permits users to access multiple applications using one set of login credentials: a zID and password. Visit Single Sign-On for guidance on SSO applications and how to sign in or out of them
- User Access Review - UNSW is required to authorise, restrict and annually verify access to UNSW information resources through conducting periodic reviews called User Access Reviews (UAR). If requested to participate in a UAR, visit User Access Review (UAR) for UAR processes, roles and responsibilities. UARs help ensure UNSW information resources are protected from fraudulent activity, unauthorised access and breaches
- System Operator Account (SA) holders - for SA account holders, visit the Password Manager for SA Accounts page for self-help guides, troubleshooting guides and FAQs about changing zID_sa passwords. The page also contains a link to the SA Password Manager self-service portal
- Privileged Access Management (PAM) - Business Owners with Privileged Access Management (PAM) can contact the IT Service Centre to request that their privileged accounts be stored and managed in the PAM service. Visit Privileged Access Management (PAM) for support materials such as the PAM user guide and FAQs. The PAM user guide contains instructions on how PAM account holders can use or manage PAM for the applications they are responsible for.

Security measures for software[36]

Due diligence should be exercised when using digital communication platforms/technologies to ensure the protection of confidential communications. Visit UNSW IT's Software for staff or Software for studying pages for instructions on how to securely install and use specific software.

[36] In clauses 2.2 (i)(n) and 6.1 of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.

In addition to these tips, visit Cyber Security Training and Awareness to learn how to deal with potential cyber security threats.

Securing personal devices[37]

Malware[38]

To assist in keeping personal devices secure, employees should avoid installing malicious applications (apps). Malicious apps are software apps designed to harm devices on which they are installed. They are capable of stealing personal information such as login credentials or payment information. To detect mobile malicious apps, employees should follow these steps:

- check the legitimacy/publisher of the app
- check the app icon for slight differences in shape and colour
- check online reviews of the app
- watch out for low numbers of downloads on apps
- be wary of extra symbols and extra words on the stated app name/developer
- check the app description name for spelling and grammar errors.

Users should contact the IT Service Centre immediately if uncertain about an app's legitimacy.

Data Stewards have an additional responsibility to ensure all UNSW Information Resources that are susceptible to malware and malicious code threats have malware detection software installed.

Phishing[39]

Users should be aware of potential phishing scams, which are designed to manipulate people into providing confidential, personal, or sensitive information. This awareness is vital for protecting UNSW information resources and digital communication platforms/technologies.

Beware of common phishing techniques including:

- urgency – This technique attempts to gather your credentials or other confidential information by presenting a financial opportunity that you must act on quickly
- threat – Messages will try to manipulate you to resolve a bogus situation. These could include some or all the following: blackmail, a financial penalty that will increase if you do not respond, or the threat that your credentials have already been compromised

[37] See clauses 5.1 – 5.6 of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.
[38] See clauses 1.8 (a), 2.2 (i) and 5.1 (b) of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.
[39] See clauses 1.8 (a), 2.1 (d) and 2.2 (h)(o) of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.

- curiosity – Fraudulent emails are crafted to attract your attention and curiosity by using a small amount of information and trying to entice you to click on a link to gather more information
- familiarity – Messages will be designed to look like a large reliable brand or appear to come from a trusted source.

Use the following methods to avoid being phished:

- independently verify phone numbers
- research the legitimacy of contact if in doubt
- verify colleague messages through alternative channels
- double-check URLs on smartphones as they are often shortened
- minimise the amount of publicly available information about you.

Password protection[40]

To assist in the protection of UNSW data, employees have a responsibility to create a strong passphrase on their personal devices. Guidance to creating a strong passphrase is as follows:

- a password (passphrase) must be a minimum of 14 characters. The passphrase should be as unpredictable and unique as possible
- each password should be different from one another. This ensures that if one password is compromised, your other accounts aren't vulnerable
- the Identity Manager portal should be used to change a zID password and perform other required functions
- many sites allow for a password to be reset if security questions are answered correctly. It is recommended that security questions with unpredictable answers are used.

Information Asset Owners and Business Owners have additional password protection responsibilities which is addressed in the Cyber Security Standard - Identity and Access Management.

For further guidance on password protection, visit UNSW Cyber Security Awareness.

Loss or theft

Employees must report the loss, theft or damage of a personal device to IT Service Centre and Campus Security. When reporting to the IT Service Centre, employees should raise a ticket and report it as a data breach.

[40] See clauses 2.2 (b) and 5.1 (a) of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.

Handling digital information

There are measures that UNSW staff can take to protect sensitive data when it is being created, shared, stored or disposed of.

Mailing lists and broadcasts[41]

Follow these recommended email practices to keep UNSW sensitive data safe:

- check UNSW email inboxes regularly for important updates
- set up devices to remotely access UNSW email accounts through a supported email application such as Outlook, or access UNSW email accounts via Outlook Web Access (OWA) on a browser
- only access UNSW email accounts on a UNSW-managed device
- only share data with others who are authorised to access it
- disable any automatic email forwarding rules in Outlook. By automatically forwarding sensitive emails to an external mailbox that does not have the same level of security as the University, there is a risk that data may be compromised, and the University may be liability for any associated privacy or security breach
- do not forward sensitive information, especially emails with a *do not forward* label
- sensitive and Highly Sensitive data should be stored on trusted platforms such as OneDrive-UNSW and SharePoint. The Cyber Security Standard - Data Security provides more guidance on the storage of UNSW data.

[41] See clauses 7.1 – 7.7 of the Use of UNSW Information Resources and Digital Communications Platforms/Technologies Procedure in the Information Governance Policy.

Section 6: Use of Artificial Intelligence (AI) systems or tools

AI is an evolving area and this manual will be periodically updated to reflect changing requirements. However, users should visit the UNSW AI Hub to keep up to date on the latest guidance on the use of AI at UNSW. The hub contains the latest advice on UNSW AI working groups, AI definitions and ethical responsibilities, as well as links to resources, training and guides.

AI self-assurance assessment[42]

An AI self-assurance assessment must be conducted before any AI system or tool is used.

As outlined in the Information Governance Policy, there are seven elements to consider as part of the assessment: **sensitive data, harm, compliance, fairness, business value, transparency & accountability, and resilience & safety.**

Details of how to complete the AI self-assurance assessment are available at the UNSW AI Hub.

Australian Government - AI Usage Guidance and Impact Assessment Tools

The following tools can be used in conjunction with the AI self-assurance assessment:

- **Voluntary AI Safety Standard** - Users are encouraged to follow the 10 AI guardrails contained in the Australian Government's Voluntary AI Safety Standard. These guardrails are voluntary and provide guidance on how to use AI responsibly.
- **The AI Impact Navigator** – Along with the 10 AI guardrails, the AI Impact Navigator's 4 dimensions should be used to measure the impact of UNSW's use of an AI system or tool.
- The Office of the Australian Information Commissioner (OAIC) has published guidance on privacy and the use of commercially available AI products. The key points users should be aware of include:
    - Privacy obligations apply to personal information input into an AI system, and to output data generated by AI that contains personal information
    - Compliance with APP 3 is required if AI systems are used to generate personal information (including images)
    - In compliance with APP 6, UNSW should only use or disclose personal information being input into an AI system for the primary purpose for which it was collected
    - Entering personal and/or sensitive information into publicly available generative AI tools is not recommended.

[42] See clauses 2.1 – 2.5 of the Use of Artificial Intelligence Systems or Tools Procedure in the Information Governance Policy.

- To ensure personal information is protected, users should take a 'privacy by design' approach to engaging with AI systems.

Human oversight[43]

Ensuring human accountability for non-operational AI systems can help build user confidence and control in an AI system. For every AI system or tool used or created at UNSW, it must be established who is responsible for:

- the use of the AI system insights/decisions
- the outcomes from the project
- the technical performance of the AI system
- data governance.

Use of AI insights/decisions

An individual should be appropriately trained on the use and limitations of an AI system or tool. This trained individual should be:

- skilled in the interpretation and critiquing of AI systems generated insights and empowered to make a decision its use.
- capable of reversing any action arising from an AI system generated insight.

Having this human oversight process is essential in cases where it is too complex to explain the factors that led to an AI system generated insight. This is because with automated systems, there is a risk of over-reliance on the generated results.

[43] See clauses 1.1 – 1.3 and 3.1 – 3.2 of the Use of Artificial Intelligence Systems or Tools Procedure in the Information Governance Policy.