Information Governance Policy

Purpose
UNSW is committed to:

- ethically and responsibly managing UNSW data, information and records
- pursuing best practice in information governance, and
- managing data, information and records in a way that meets UNSW’s legal, risk, environmental, business, teaching, learning and research requirements.

The purpose of this policy is to:

- provide a comprehensive set of enterprise-wide principles and procedures 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
- ensure UNSW complies with applicable laws, standards, codes, guidelines, ethics approvals and contractual obligations in relation to information governance.

Scope
This policy applies to:

- all information collected, used or generated at UNSW or during UNSW-affiliated research in accordance with the University's functions, including published research data, unpublished research data, research materials, master data, reference data, metadata, and records
- all formats of data, information and records including print, electronic, audiovisual or any other format
- UNSW information resources (including for example, procured library and scholarly information resources)
- digital communication platforms/technologies
- artificial intelligence systems and tools
- all devices connected to a UNSW network or used to access UNSW information resources.

This policy applies to all members of the UNSW community, which comprises all students, researchers, research trainees, employees, affiliates and contractors/consultants. The procedures that follow the policy may state that a more limited scope applies.

Information Governance Policy ................................................................................................................................. 1
Section 1: Data Management Procedure ...................................................................................................................... 6
Section 2: Records and Information Management Procedure ..................................................................................... 16
Section 3: Privacy Procedure ........................................................................................................................................ 20
Section 4: Data Breach Procedure .............................................................................................................................. 22
Section 5: Use of Information Resources and Digital Communications Platforms Procedure ...................................... 26
Section 6: Use of Artificial Intelligence Systems or Tools Procedure ........................................................................... 33

Principles and objectives

1. Data management

1.1. Data is a strategic asset of UNSW. It is therefore critical for UNSW to have appropriate governance
for the management and effective use of its data.

1.2. Data is managed throughout its life cycle in compliance with this policy and, where relevant, ethics approvals, codes, guidelines, third-party agreements and applicable legislation.

1.3. UNSW implements robust and effective data management practices to control the integrity, security, quality, use and reuse of data (and metadata).

1.4. Data is protected against unintentional and/or unauthorised modification, including unauthorised destruction and misuse, as well as internal and external threats.

1.5. Access to and the transmission, use and sharing of UNSW data within UNSW and externally are governed and documented by an approved agreement.

1.6. UNSW secures, protects and retains data for future use in an accessible, auditable and traceable manner in accordance with applicable retention periods.

1.7. Where permissible and possible, research data is shared and disseminated to maximise its value, encourage collaboration and foster research and teaching innovation.

1.8. Aboriginal and Torres Strait Islander peoples’ data is managed in accordance with their rights and interests and any relevant ethics approvals, codes, guidelines, third-party agreements and applicable legislation.

2. Records and information management

2.1. UNSW’s records are UNSW’s corporate memory. They:

- provide evidence of actions and decisions
- are vital assets that support daily functions and operations
- protect the interests of UNSW and the rights of the UNSW community and the people of New South Wales
- help UNSW deliver services consistently and equitably
- are part of the intellectual property and cultural heritage of New South Wales.

2.2. Records must always be:

- created and captured to document UNSW business activity
- captured to a UNSW System of Record
- discoverable across UNSW by those with legitimate need and appropriate access for as long as required
- accurate, up to date and complete, and never destroyed without written approval.

2.3. UNSW Systems of Record protect records from unauthorised access, alteration, deletion or misuse, and ensure that UNSW records retain value as evidence.

2.4. Records and information management practices support good decision-making, accountability and transparency to deliver best practice business outcomes.

2.5. Records and information management is a component of all processes, systems and services, and ownership of records is always defined and allocated.

2.6. Records are kept for as long as they are needed for business and legal accountability (including in accordance with retention and disposal authorities) and to meet community expectations.

2.7. Records are always retained according to current State Records NSW retention and disposal authorities and are accountably destroyed when appropriate. Sentencing records maps them directly to a record class and defines their minimum retention requirements.

2.8. Records are disposed of and destroyed according to the Records and Information Management procedure.
3. **Privacy**

3.1. Privacy is embedded into the design of all UNSW systems, services and practices.

3.2. UNSW collects, holds, uses and discloses personal and health information by lawful, fair and transparent means in compliance with this policy, the UNSW Privacy Management Plan, relevant UNSW Privacy Statements, and applicable ethics approval, codes, guidelines, third-party agreements and legislation in respective jurisdictions.

3.3. Where UNSW collects and holds personal and health information, it is only collected, held and used for the purposes and consent for which the information was collected.

3.4. UNSW takes reasonable steps to ensure the personal and health information it holds is up to date, accurate and relevant to the purpose for which it was collected.

3.5. Personal and health information collected and held by UNSW can, where appropriate, be accessed and, on request, changed by the person to whom the personal and health information relates.

3.6. UNSW protects the security of personal and health information against internal and external threats through de-identification and by regularly assessing the risk of unauthorised or unlawful use, disclosure, interference, accidental loss and damage.

3.7. Personal and health information collected and held by UNSW is disposed of in a secure manner in accordance with this policy and applicable legislation.

4. **Data breaches**

4.1. UNSW complies with its legislative obligations to protect data, avoid or reduce possible harm to affected individuals and UNSW, and prevent future breaches.

4.2. Data breaches are reported internally as soon as they are identified.

4.3. The Data Breach Management Procedure section below includes a Data Breach Management Plan, which UNSW uses to assess and manage data breaches systematically.

4.4. UNSW notifies individuals and entities affected by a data breach in accordance with legislative obligations.

4.5. UNSW records data breaches and monitors, analyses and reviews the type and severity of suspected data breaches and the effectiveness of its response.

5. **Use of UNSW information resources and digital communication platforms/technologies**

5.1. UNSW information resources and digital communications platforms/technologies are used lawfully, ethically and responsibly.

5.2. UNSW information resources and digital communication platforms/technologies are used in compliance with this and other UNSW policies and applicable legislation.

5.3. Users of UNSW information resources and digital communications platforms/technologies are responsible for their personal UNSW accounts, or other UNSW accounts that they use, as well as any digital information they store, process or transmit using, or while connected to, a UNSW information resource.

5.4. Users of UNSW information resources and digital communications platforms/technologies take all reasonable steps to protect UNSW information resources from physical or digital theft, damage or unauthorised use.

5.5. UNSW provides access to UNSW information resources and digital communication platforms/technologies for users to perform legitimate work, research or studies at UNSW and all use is consistent with that purpose.
6. **Use of AI systems or tools**

6.1. The use of artificial intelligence (AI) has the potential to benefit UNSW, individuals, society and the environment.

6.2. AI is used equitably with respect for human rights and diversity and to foster inclusion and accessibility.

6.3. AI systems or tools are trustworthy and are used responsibly, safely and reliably in accordance with their intended purpose throughout their life cycle.

6.4. The use of AI is transparent and people understand when AI is engaging with or affecting them and/or the environment.

6.5. AI systems or tools used at UNSW are identifiable, explainable, interpretable, accountable and contestable throughout their life cycle.

6.6. AI systems or tools used at UNSW are secure and resilient throughout their life cycle.

7. **Responsibilities**

7.1. The Information Governance Steering Committee (IGSC) oversees UNSW-wide information governance and provides oversight and assurance of related strategic initiatives to protect data, information and records across UNSW.

7.2. The Information Governance Ethics Advisory Group provides advice to the IGSC on the ethics of all data use (other than research data).

7.3. The Research Ethics and Compliance unit provides advice to the IGSC on the ethics of research data use.

7.4. The Research Data Management Steering Committee oversees the governance and management of research data on behalf of the IGSC.

7.5. The Enterprise Data Governance and Management Steering Committee oversees the governance and management of data on behalf of the IGSC.

7.6. The University Leadership Team are responsible for:

- overseeing the management of personal and health information within their respective portfolios
- nominating a University Compliance Owner (UCO) for personal and health information held within their portfolio, while remaining responsible for the performance of the UCO’s duties, which are set out in the Privacy procedure section below.

7.7. The Chief Information Officer has UNSW-wide authority to:

- establish mandatory standards and guidelines and determine the consultation process (in accordance with the [UNSW Policy Framework Policy](#)) including the authority to expedite changes to facilitate the management of high or extreme cyber security risks
- decide whether work, use of equipment, or an operation must cease due to identified or perceived cyber security risk or a major incident caused by that activity
- assign UNSW-wide management responsibilities for the use of
  - UNSW information resources
  - digital communication platforms/technologies
  - artificial intelligence systems.

7.8. The Chief Data & Insights Officer is responsible for the overall management of UNSW’s data governance and data management, and:

- defining and implementing an enterprise data analytics and management strategy

7.9. The Manager, Records & Archives is responsible for the oversight of UNSW records and information, and:
• overall management of UNSW’s records and information
• measuring the performance of UNSW against the Records and Information Management procedure section below
• maintaining the Records and Information Management Procedure and the Information Governance Instruction Manual
• leading records and information management initiatives
• collaborating with other relevant stakeholders to ensure best practice records and information practices are embedded across UNSW
• working with other accountable stakeholders, including auditors, Government Information (Public Access) (GIPA) officers, and executive management to ensure that systems that manage records and information support organisational and public accountability.

7.10. The General Counsel has authority to change the:
• Privacy Procedure
• Data Breach Procedure
• Information Governance Instruction Manual.

8. Compliance with this policy

8.1. Where a person suspects that serious wrongdoing has occurred, including corrupt conduct, serious maladministration, a government information contravention, a privacy contravention, and/or a serious and substantial waste of public money, they must report this in accordance with the Public Interest Disclosure (Whistleblowing) Policy and Procedure.

8.2. Researchers must report potential breaches of the Australian Code for the Responsible Conduct of Research.

8.3. Non-compliance with this policy may constitute a breach of the UNSW Code of Conduct and Values.
Section 1: Data Management Procedure

Scope
This procedure applies to all data collected, used or generated at UNSW or during UNSW affiliated research projects or research activities in accordance with the University’s functions, including published research data, unpublished research data, research materials, master data, reference data, and metadata.

Data management life cycle
Every data element must be managed throughout its life cycle, where appropriate, in accordance with ethics approvals, codes, guidelines, third-party agreements and applicable legislation.

The data management life cycle at UNSW comprises the following phases:

- **Plan and design** – management of data is planned and designed to meet UNSW’s needs and compliance requirements throughout the data life cycle.
- **Create, collect and classify** – data is accurately created or captured (with permission when relevant), and classified and metadata is recorded. Where appropriate, data is cleansed.
- **Organise, store and secure** – data is stored appropriately and securely in accordance with its data classification and confidentiality risk rating.
- **Manage and maintain** – data is managed to maintain its integrity, quality and usability.
- **Share and (re)use** – data is discoverable, accessible, and shared where appropriate for (re)use. This phase also includes the publication of research data and materials.
- **Retain** – data is retained in accordance with relevant retention requirements.
- **Dispose and destroy** – data is appropriately disposed of and destroyed.

This lifecycle is aligned with the National Institute of Standards and Technology (NIST) Research Data Lifecycle and the Australian Research Data Commons (ARDC) Research Data Management Framework.
1. **Plan and design**

   1.1. Every data element must be linked to:

      a. a **Data Custodian** who is responsible for the oversight and management of the data delegated to them, and

      b. a **Data Steward** who is responsible for the quality and integrity, ethics, implementation and enforcement of data management within their business unit or research project.

   1.2. This information must be captured as a record in a data management plan.

   1.3. The **Data Custodian** must assign each data element a **data domain**.

   1.4. The **Data Custodian** must create a data management plan for each non-research data domain. The plan must be maintained and adhered to throughout the data management life cycle.

   1.5. For each research activity or project, the researcher must create a research data management plan in consultation with the **Data Custodian**. The plan must be maintained and adhered to throughout the data management life cycle.

   1.6. Metadata must be described and documented in each data management plan by the **Data Custodian** and managed throughout the data management life cycle.

2. **Create, collect and classify**

**Data creation or collection**

   2.1. Data should only be created or collected in accordance with the data management plan to fulfil the University’s functions.

   2.2. Data must be accurate, valid and complete at the time of creation or collection.

   2.3. Data **Custodians** must ensure that any data being created or collected (other than research data) complies with:

      a. the Data Ethics Guideline, and

2.4. To ensure accuracy, data should be collected and recorded immediately or in real time, where possible, after the event or activity.

2.5. Data created or collected outside a UNSW campus must be transported to a UNSW campus or transmitted to a UNSW information resource, unless an agreement specifies otherwise.

2.6. The collection of data outside Australia must comply with the data collection laws of that jurisdiction. For example, personal data collected from European Union citizens must comply with the requirements of the General Data Protection Regulation (2016/679).

2.7. For the types of data listed in the box below, the following additional data collection procedures must be followed:

### Research Data
Data Custodians must ensure that research data being created or collected complies with ethics approvals; UNSW’s Privacy Management Plan; relevant UNSW Privacy Statements, codes, guidelines and third-party agreements; and the Australian Code for the Responsible Conduct of Research.

Researchers collecting research data and materials via data entry or surveys should use UNSW approved tools as set out in Appendix 2: Information Governance Instruction Manual, where possible.

In addition:

- **Human research data**
  Human research data must be created or collected in compliance with the UNSW Human Research Ethics Procedure and the NHMRC Management of Data and Information in Research.

  Researchers collecting research data from human participants must do so in compliance with the principles of the NHMRC National Statement on the Ethical Conduct in Human Research and applicable legislation and standards.

- **Animal research data**
  Research data from animals must be created or collected in compliance with the UNSW Animal Research Ethics Procedure.

  Researchers collecting research data from animals must do so in compliance with the principles of the NHMRC Australian code for the care and use of animals for scientific purposes and applicable legislation and standards.

### Aboriginal and Torres Strait Islander peoples
Aboriginal and Torres Strait Islander peoples’ data must be created or collected in compliance with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research and the NHMRC Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities.

Researchers engaging in fieldwork in areas of significance to Aboriginal and Torres Strait Islander peoples must acknowledge, consult, and engage with the Indigenous owners of the land before commencing fieldwork.

### Personal and/or health information
Personal and/or health information must be collected in compliance with UNSW’s Privacy Management Plan and relevant Privacy Statements.

### Data classification
2.8. The Data Custodian (in collaboration with the researcher where appropriate) is required to classify each data element for which they are responsible in accordance with the UNSW Data Classification Standard and, where appropriate, any relevant classification requirements stipulated by state/federal legislation, funding bodies and/or data providers.
2.9. Once the data element is classified, the Data Custodian (in collaboration with the researcher where appropriate) must assign it a confidentiality risk rating in accordance with the Cyber Security Standard – Data Security.

2.10. Following assignment of the confidentiality risk rating the Data Custodian (in collaboration with the researcher where appropriate) must determine the respective Dissemination Limiting Marker in accordance with the procedures set out in Appendix 2: Information Governance Instruction Manual.

2.11. Data Custodians must conduct regular audits of data classification and data security compliance.

2.12. Where a data element’s original classification has changed, it must be re-classified throughout the data management life cycle. The new classification must be recorded by the Data Custodian in the relevant data management plan.

3. Organise, store and secure

Data cleansing

3.1. Unnecessary duplication of data across IT services, devices, and storage locations including hard copies, must be avoided.

3.2. Data cleansing includes detecting and correcting data errors to improve the quality of data.

3.3. All data (other than research data) must be cleansed routinely via an automated process where possible, in accordance with the Data Quality Guideline as set out in Appendix 2: Information Governance Instruction Manual.

Data storage

3.4. Data that constitutes a record must be stored in a UNSW System of Record in accordance with the Records and Information Management procedure section below. Data that does not constitute a record must be stored in a UNSW approved storage platform in accordance with Appendix 2: Information Governance Instruction Manual.

3.5. Data storage must be secure, appropriate to the classification and confidentiality risk rating of the data, and comply with legal, ethical and funding requirements.

3.6. The Data Custodian (in collaboration with the researcher where appropriate) must determine the appropriate storage platform for the data.

3.7. Data in digital format must be stored in an appropriate, secure location in accordance with the Cyber Security Standard – Data Security.

3.8. Data in physical format should always be stored securely with appropriate access restrictions.

3.9. Portable storage devices storing medium or high confidentiality risk rated UNSW digital information must be backed up to a cloud preferred drive or to a duplicate device if a network drive is not possible, in accordance with the Cyber Security Standard – Data Security.

3.10. Portable storage devices of an unknown source or origin must not be used.

3.11. In accordance with the Cyber Security Standard – Data Security, digital information must not be stored unencrypted on any personal computer, cloud storage or external drive.

3.12. For the types of data listed in the box below, the following additional procedures must be followed:

<table>
<thead>
<tr>
<th>Research Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research data must be stored in a UNSW-supported information system, onsite at UNSW or in an approved research system, where possible.</td>
</tr>
</tbody>
</table>
When an information system not supported by UNSW is used to store research data, the Data Custodian must, in collaboration with the researcher, ensure that the unsupported platform meets UNSW cyber security requirements and the third-party service provider is subject to a legally binding agreement with UNSW to ensure data security and protection from unauthorised access, use or disclosure. A research data risk assessment of the unsupported platform must be undertaken, and a written record of the platform must be documented in the Research Data Management Plan.

Physical research materials must be stored in the relevant faculty and, where possible, digitised.

Researchers should consider whether research materials (including specimens or samples) should be retained in research repositories such as a specified museum, Cold Storage, or the UNSW Herbarium in accordance with the procedures set out in Appendix 2: Information Governance Instruction Manual.

Aboriginal and Torres Strait Islander people’s data
Aboriginal and Torres Strait Islander peoples’ data must be stored in compliance with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research and in consultation with the Aboriginal and Torres Strait Islander owners of the data. Prior to data procurement, researchers, community members and partnering organisations should formally document agreement on the storage, dissemination and potential secondary use of data.

Personal and/or health information
Personal and/or health information must be stored in compliance with UNSW’s Privacy Management Plan and relevant Privacy Statements.

4. Manage and maintain

4.1. The Data Custodian and Data Steward must manage and maintain the data, where appropriate and plausible, throughout its life cycle.

4.2. Data Stewards must review and revise the accuracy, completeness, consistency, timeliness, integrity and validity of all data (other than research data) on a regular basis in accordance with the Data Quality Guideline and the Data Ethics Guideline.

4.3. Data Custodians must ensure that data management plans are updated and regularly reviewed.

4.4. Data Stewards must ensure that metadata is appropriately measured, monitored and subject to quality and assurance audits throughout the data management life cycle.

4.5. For the types of data listed in the box below, the following additional procedures must be followed:

Research Data
Data Custodians must ensure that the management of data complies, where required, in accordance with the relevant UNSW ethics approval procedure; UNSW’s Privacy Management Plan and relevant Privacy Statements; codes, guidelines, third-party agreements and the Australian Code for the Responsible Conduct of Research.

Researchers must report any risk of harm to humans, animals or the environment to UNSW Research Ethics and Compliance Support as soon as possible.

Aboriginal and Torres Strait Islander people’s data
Aboriginal and Torres Strait Islander peoples’ data must be managed and maintained in compliance with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research.
5. Share and (re)use

Data sharing

5.1. UNSW data must not be accessed, viewed, shared or used by anyone from outside the business unit that is responsible for managing the data without data sharing approval or other written approval from the relevant Data Custodian. The sharing of data must accord with the classification of the data.

5.2. UNSW data must not be shared with an external third-party (including product vendors, service providers, consultants and accreditation or industry bodies) without the third-party entering into a legally binding agreement with UNSW to ensure data security and protection from unauthorised access, use or disclosure.

5.3. Where appropriate, before any data (other than publicly available data) is shared outside UNSW, the Data Steward must verify the data to ensure its quality, integrity and security will not be compromised.

5.4. The process for obtaining data sharing approval is set out in Appendix 2: Information Governance Instruction Manual. Further information and resources are located on the Information Governance Intranet.

5.5. The Information Governance and Assurance Office may conduct regular reviews of data sharing compliance and take action to address any non-compliance.

5.6. For the types of data listed in the box below, the following additional procedures must be followed:

### Research Data

Unpublished research data must not be shared within UNSW or externally without ethics approval or data sharing approval.

Unpublished research data containing personal information must not be shared within UNSW or externally without the written consent of the individuals concerned and ethics approval or data sharing approval.

A researcher must not take research data to another university unless a written agreement is in place with the researcher’s new organisation covering ownership, use, storage and disposal of the research data.

### Data transmission

5.7. UNSW data must only be transmitted in accordance with the Cyber Security Standard – Data Security and any relevant data sharing approval or other relevant legal instrument.

5.8. Data that has a ‘medium’ confidentiality risk rating must be encrypted in transit when transmitted through public or untrusted networks in accordance with the algorithms and protocols in the Cyber Security Standard – Data Security.

5.9. Data that has a ‘high’ confidentiality risk rating must be:

   a. encrypted when transmitted through public or untrusted networks and public cloud environments in accordance with the algorithms and protocols in the Cyber Security Standard – Data Security and

   b. have encryption keys managed in accordance with the key management requirements in the key and certificate management requirements in the Cyber Security Standard – Data Security.
5.10. UNSW Legal & Compliance must conduct a Privacy Impact Assessment before data (that is not subject to a data sharing agreement or other binding legal agreement) that contains personal information or health information about an individual is transferred outside New South Wales or to a Commonwealth agency.

5.11. 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 or their delegate for additional control requirements.


Data access, use and re-use

5.13. UNSW data is held and controlled by UNSW not by any individuals. This does not however prevent its (re)use.

5.14. Data must be used only in accordance with its data and security classification and only for the purpose(s) for which it was collected.

5.15. Access to data must be granted on a least privilege and need to know basis, in accordance with the Cyber Security Standard – Identity and Access Management.

5.16. Personal use of data (other than research data) is prohibited.

5.17. Access to and the (re)use of data must be recorded in the data management plan.

5.18. For the types of data in the box below, the additional procedures stated must be followed, where relevant:

---

**Research Data**

Research data is held and controlled by UNSW, unless subject to a third-party licence agreement, research data sharing agreement or in respect of intellectual property as defined by the Intellectual Property Policy and the Research Authorship, Publication and Dissemination Policy.

UNSW is committed to open access to research data, as a Group of Eight member and signatory of the Sorbonne Declaration on Research Data Rights.

Data Custodians must ensure that the open access requirements of the UNSW Open Access Policy, the Australian Code for the Responsible Conduct of Research 2018 and funding bodies including the Open Access Policy of the Australian Research Council and the Open Access Policy of the National Health and Medical Research Council are met.

Researchers should, in consideration of privacy, copyright, intellectual property, ethics, cultural sensitivities, third-party and data sharing agreements, encourage open access to research data.

Researchers must make their data available upon request by UNSW e.g. when integrity concerns or staff misconduct arises.

Researchers using existing unpublished research data to inform their research project must have permission and meet the conditions for re-use, including the retention and disposal requirements. Unless new research data and information is derived, and therefore new retention requirements arise, avoid unnecessary duplication and retention of existing data.

---

**Aboriginal and Torres Strait Islander people’s data**

Aboriginal and Torres Strait Islander peoples have sovereignty and ownership of research data related to their people, culture, and practices, in line with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research.

Access to and the (re)use of UNSW data relating to Aboriginal and Torres Strait Islander people must pertain to what has been ethically approved by the reviewing Human Research Ethics Committee, and in consultation with the Aboriginal and Torres Strait Islander owners of the data.
Personal and/or health information

Access to and the (re)use of personal and/or health information must comply with UNSW’s Privacy Management Plan and relevant Privacy Statements.

6. Data retention

6.1. Data that constitutes a record must be retained in accordance with the Records and Information Management Procedure section below.

6.2. Data that does not constitute a record must be retained in accordance with the procedures set out in Appendix 2: Information Governance Instruction Manual.

6.3. For the types of data in the box below, the additional procedures stated must be followed, where relevant:

**Research Data**

Researchers have primary responsibility for determining and applying the appropriate retention period for their research data and materials, including long-term retention. Such decisions should be made in collaboration with Data Custodians.

Researchers leaving UNSW must ensure that research data is retained by UNSW to support research integrity and fulfil retention obligations.

Researchers must publish metadata about their research that is published or made publicly available in association with a project, publication, or HDR thesis in UNSWorks, the UNSW institutional repository, and the data accessible via UNSWorks or a suitable third-party repository.

**Aboriginal and Torres Strait Islander people’s data**

Data that may have cultural significance or value to Aboriginal and Torres Strait Islander peoples’ decision-making should be retained for future use in accordance with Indigenous data governance principles.

UNSW must retain Aboriginal and Torres Strait Islander peoples’ data in compliance with the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research and in consultation with the Aboriginal and Torres Strait Islander owners of the data.

**Personal and/or health information**

Personal and/or health information must be retained in compliance with UNSW’s Privacy Management Plan and relevant Privacy Statements.

7. Data disposal and destruction

7.1. Data that constitutes a record must be disposed of and destroyed in accordance with the Records and Information Management procedure.

7.2. Data that does not constitute a record must be disposed of and destroyed in accordance with the procedures set out in Appendix 2: Information Governance Instruction Manual.

8. Roles and responsibilities

8.1. The Chief Data & Insights Officer
See the responsibilities section of the Information Governance policy above for the responsibilities and authorities of the Chief Data and Insights Officer, which include enterprise data governance and management activities.

8.2. **Information Governance and Assurance Office**

The Information Governance and Assurance Office supports the Chief Data & Insights Officer to maintain and implement the principles and procedures in relation to information governance. The office is responsible for:

- ensuring that key information governance roles are appointed, inducted and are aware of their responsibilities
- providing information governance training and deliver awareness initiatives to the UNSW community as required, to improve information literacy and awareness across UNSW
- responding to information governance legislative and regulatory requirements
- responding to committees on information governance assurance and compliance as required
- undertaking initiatives to enhance data life cycle management at UNSW.

The Information Governance and Assurance Office can be contacted via email at datagov@unsw.edu.au.

8.3. **Data Executives**

Data Executives are senior leaders with planning and decision-making authority for a specific data domain. The role provides high-level oversight of data and data quality for the data domain. It also serves as an escalation point to resolve any matters that are unable to be resolved by the Data Custodians and Data Stewards for a data domain.

The Data Executives, as a group, are responsible for overseeing the continuous improvement of UNSW’s data governance and management.

Data Executives are delegated by the Information Governance Steering Committee and in turn delegate day-to-day accountability for the data assigned to them to Data Custodians and Data Stewards.

A list of the Data Executives at UNSW is set out in the Information Governance Instruction Manual.

8.4. **Data Custodians**

Data Custodians are business leaders with day-to-day accountability for oversight and management of one or more data domains delegated to them by a Data Executive. For example, the Head of HR Systems is the Data Custodian for the human resources domain. Heads of Schools, Heads of Research Institutes, Chief Investigators and/or Principal Investigators, and supervisors may be the Data Custodian for the research domain. Heads of Schools (or Chief Investigators or Principal Investigators) are responsible for maintaining a register of confidential information.

For each assigned domain, the Data Custodian is responsible for:

- key data management decisions and directions
- ensuring that specific industry or research requirements (e.g. Australian Code for the Responsible Conduct of Research, Payment Card Industry Data Security Standard) are identified within their assigned domains, and that appropriate controls are implemented
- reviewing and approving data sharing approvals; and the quality and integrity, ethics, implementation and enforcement of data management.

Data Custodians are responsible for ensuring research data and materials have continuous custodianship and, when people with a role or responsibility in a research project leave UNSW, should appoint an appropriate replacement (in consultation with the Data Steward).
A list of the Data Custodians at UNSW is set out in the Information Governance Instruction Manual. N.B. The list does not include Data Custodians responsible for research at UNSW.

8.5. Data Stewards
Data Stewards are functional or operational leaders who represent a business unit related to a specific data domain. Every data domain (including research projects) must have one or more Data Stewards. Data Stewards are responsible for the quality and integrity, ethics, implementation and enforcement of data management within their business unit.

A list of the Data Stewards at UNSW is set out in the Information Governance Instruction Manual. N.B. The list does not include Data Stewards responsible for research at UNSW.

8.6. Data users
Data users are members of the UNSW community who use data that they have been granted access to for authorised purposes to carry out their day-to-day duties.

Data users are responsible for:

- using data in compliance with this policy and relevant legislation
- using data ethically and securely while respecting confidentiality and privacy
- ensuring the data they consume is fit for its specific purpose/s, and
- providing feedback about the quality of data to relevant Data Stewards.

8.7. External data users
External data users are persons or organisations who access, input, amend, delete, extract, or analyse data and the information created by data in/from a UNSW information resource and are not employees, contractors, consultants or authorised agents of UNSW. For example, vendors of information systems and information services used by UNSW are external data users.

Effective: [XX Month] 2024   Responsible: xxxxx   Lead: xxxxx
Section 2: Records and Information Management Procedure

Scope
This procedure applies to employees, affiliates and contractors/consultants.

1. Systems

1.1. Records must be captured to a UNSW System of Record. These are business systems that have been assessed to ensure the requirements of a record are met.

   A UNSW System of Record must be:
   • a system that is managing UNSW records such as RAMS (Records and Archives Management System)
   • capable of meeting any legislative requirements for these records
   • able to capture (and return) fixed, complete, authentic, reliable, useable records
   • able to capture (and show) core metadata (description, structure, context, related records, events, retrieval information) during and beyond the life of the record itself
   • secure and able to restrict access to records (and metadata) or groups of records to meet accountability, legislative and business requirements
   • able to prevent deletion of records and metadata unless as part of authorised disposal activity
   • able to capture an audit log of system activity
   • able to support migration and/or controlled disposal of records depending on the period for which records must be retained
   • authorised as a UNSW System of Record, have an identified records and information management (RIM) Steward and (RIM) Custodian.

1.2. The assessment process for a UNSW System of Record is to be completed by the RIM Steward using this form and is maintained by the Records & Archives Office.

1.3. Records and information management is assessed and addressed by the RIM Steward in all outsourced, cloud and similar service arrangements.

1.4. The RIM Steward must ensure that records and information are maintained throughout system and service migrations.

1.5. System decommissioning takes into account retention and disposal requirements for records and information held in the system before final approval by the Manager, Records & Archives.

2. Long-term records

2.1. State archives and University archives are routinely identified and transferred by the Records & Archives Office to safeguard, manage and preserve records with long-term value.

2.2. Records that are more than 20 years old are by default under the State Records Act NSW (1988) deemed to be open to public access unless a CPA (Closed to Public Access) direction has been made by UNSW. CPAs are created and maintained by the Records & Archives Office.
3. Assurance and compliance with NSW State Archives, State Records NSW and Museums of History NSW requirements

3.1. The Records & Archives Office:
- conducts regular reviews of compliance with the requirement to identify and preserve NSW State archives
- routinely monitors and reviews records and information assets to ensure business needs are met and compliance with the State Records Act and codes of best practice
- routinely monitors and reviews compliance with State Records NSW and Museums of History NSW
- routinely monitors and reviews systems to ensure the integrity, useability and accessibility of records and information.

4. Storage and scanning

4.1. Records and information in digital format must be stored in an appropriate, secure location in accordance with the Cyber Security Standard – Data Security. Hard copy records should always be stored securely with appropriate access restrictions.

4.2. Portable storage devices storing medium or high Confidentiality Risk rated digital information must comply with the Cyber Security Standard – Data Security.

4.3. Portable storage devices of an unknown source or origin must not be used.

4.4. Records stored offsite should use UNSW’s preferred supplier of storage. Records stored offsite must always be appraised and a disposal authority applied prior to their transfer.

4.5. Scanning records from hardcopy to digital only impacts their format; it has no bearing on the minimum legal period for which they must be retained. However, it may be possible to destroy the source paper records as part of this process if the conditions for their destruction have been met.

4.6. The Records & Archives Office routinely monitors and reviews compliance with record storage requirements.

5. Retention and disposal

5.1. Records must never be destroyed by the RIM Custodian without undergoing a formal process of appraisal, and consultation where appropriate with the researcher and the approval of the Records & Archives.

5.2. Once the destruction of record is approved, the RIM Custodian must ensure that the records are securely and irretrievably destroyed.

5.3. Records that are ephemeral or facilitative and do not have any continuing value are destroyed in accordance with Normal Administrative Practice (NAP). What constitutes NAP is described here, https://www.recordkeeping.unsw.edu.au/recordkeeping/normal-administrative-practice-nap

5.4. The Records & Archives Office monitors and reviews compliance with record retention and disposal requirements.

6. High risk and high value records

6.1. UNSW is required to identify the systems, records and information needed to support its’ high value and high-risk processes.

6.2. High risk and high value records are one (or more) of the following:
- records UNSW is required to retain for more than 20 years
- records of UNSW’s core activities (research, teaching)
- records of UNSW’s key corporate functions (personnel, finance, student administration)
• records containing personal or health information
• records of agreements and contracts for expenditure of $150,000 or more (including GST)
• records of significant organisational change.

6.3. Records of high-risk high value business and the systems that manage them are identified and documented by the Records & Archives Office to enable them to be prioritised and any risks evaluated and managed appropriately.

6.4. A UNSW System of Record assessment is used by the Records & Archives Office to identify where records of high-risk high value business are captured. The completion of these evaluations is the responsibility of the RIM Custodian.

6.5. RIM Stewards retain overall responsibility for ensuring records of high risk and high value business are safely managed and protected by business continuity plans.

6.6. A Register of High Risk and High Value business and the systems that manage them is maintained by the Records & Archives Office.

6.7. The Records & Archives Office routinely monitors and reviews compliance with the requirements for the identification and management of high-risk records.

7. Metadata records

7.1. The following metadata must be recorded for records and information:

a. a description of their content

b. their structure (form and format) and the relationships between their components which comprise them

c. the business context in which they were created or received and used; who created them, why they were created, how they have been used and managed

d. relationships with other records, information and metadata

e. business actions and events involving the records and information throughout their existence

f. information that may be needed to retrieve and present them.

7.2. Metadata must be configured in systems and carried forward to accompany the records through system changes.

8. Roles and Responsibilities

8.1. Manager, Records & Archives

See the responsibilities section of the Information Governance policy above for the responsibilities and authorities of the Manager, Records & Archives.

8.2. Records & Archives Office

The Records & Archives Office supports the Manager, Records & Archives to maintain and implement the principles and procedures in relation to records and information management. The Office is responsible for:

• support for the management of all records, in any format, including access to and use of the enterprise recordkeeping system RAMS

• providing records and information management training and initiatives to the UNSW community as required, to improve records and information management practice across UNSW

• the collection, maintenance and provision of access to, UNSW’s archival collections
• consultancy services on records and information management including business process analysis, redesign and support for the identification of digital recordkeeping solutions
• oversight of the UNSW System of record framework
• providing advice on, and authorisation for, the disposal of records
• responding to records and information management legislative and regulatory requirements.

8.3. Records and Information Management (RIM) Stewards

RIM Stewards retain responsibility for ensuring that:

• appropriate systems and processes are in place for capturing, storing and disposing of records within their areas of responsibility
• employees in their business unit are aware of their recordkeeping responsibilities
• UNSW Systems of Record are available within their areas for the capture and management of records and that any new systems or process are assessed prior to implementation
• their employees are aware of the need to appraise records before destruction and to never destroy records without the necessary approval
• high risk and high value business records and the systems which manage them are identified and responsibility for capturing and managing these records is assigned.

8.4. Records and Information Management (RIM) Custodians

RIM Custodians are responsible for:

• the records and information managed by the business systems and/or processes for which they have been assigned custodianship
• identifying the records of their Unit’s activities, and ensuring the appropriate capture, storage, classification and disposal of these records
• ensuring systems managing high risk and high value business records are protected by business continuity strategies and plans
• ensuring employees are aware of their recordkeeping responsibilities and how to meet them.

Effective: [XX Month] 2024  Responsible: xxxxx  Lead: Manager, Records & Archives
Section 3: Privacy Procedure

Scope
This procedure applies only to the UNSW community. Controlled entities of UNSW manage personal and health information in accordance with laws applicable to that entity.

1. UNSW Privacy Management Plan
   1.1. UNSW manages personal and health information in accordance with this policy and the Privacy Management Plan.

2. Privacy impact assessments
   2.1. Before any new project (other than a research project or activity) that is designed to hold or process personal information and/or health information on behalf of UNSW is implemented, it may be subject to a Privacy Impact Assessment (PIA). A PIA ensures that personal information and/or health information is protected from unauthorised access, use, modification or disclosure.
   
   2.2. The sponsor of the new project is responsible for notifying UNSW Legal & Compliance and, where appropriate the UNSW IT Cyber Security Strategy & Governance team, that a new project has been proposed.
   
   2.3. The procedure for conducting a PIA is set out in Appendix 2: Information Governance Instruction Manual.
   
   2.4. UNSW Legal & Compliance will advise the new project sponsor of the outcome of the PIA assessment.

3. Right to information
   
   3.1. UNSW publishes open access information that can be accessed via the Accessing University Information webpage or by conducting a search of UNSW’s website at https://www.unsw.edu.au/
   
   3.2. UNSW may disclose information that is not published on its website informally or through a formal application process in accordance with the Government Information (Public Access) Act 2009 (NSW).
   
   3.3. Informal requests for information should be emailed to: gipaa@unsw.edu.au
   
   3.4. The procedure for requesting information is set out in Appendix 2: Information Governance Instruction Manual.

4. Privacy complaints
   
   4.1. Privacy complaints about UNSW may be resolved through the Complaints Management and Investigations Policy and Procedure, or through an application for internal review under the Privacy and Personal Information Protection Act 1998 (NSW) (PIPP Act). Further information about internal or external complaints is set out in the Privacy Management Plan.
   
   4.2. The procedure for making a privacy complaint is set out in Appendix 2: Information Governance Instruction Manual.
5. Roles and responsibilities

5.1. University Leadership Team
See the responsibilities section of the Information Governance policy above for the responsibilities and authorities of the University Leadership Team.

5.2. UNSW Legal & Compliance
UNSW Legal & Compliance is responsible for:
- providing advice on the privacy obligations imposed by this policy and applicable privacy laws.
- supporting the University Compliance Officers to develop local protocols and privacy statements for use in their area of responsibility
- developing guidelines, training and other supporting material to support awareness of obligations imposed by applicable privacy laws
- conducting internal reviews of privacy complaints received in accordance with applicable legislation.

5.3. University Compliance Owners (UCOs)
UCOs are responsible for:
- ensuring that University-wide procedures implemented to support this policy are applied in the management of personal and health information within their respective portfolios
- implementing effective local procedures to ensure that personal and health information held within their portfolio is managed in accordance with this policy
- ensuring that any person who has access to the personal information held within their portfolio understands their responsibilities regarding such information
- ensuring that privacy statements that comply with all applicable laws are provided to individuals when their personal information is collected.

Effective: [XX Month] 2024  Responsible: xxxxx  Lead: Head of Compliance & Privacy Law
Section 4: Data Breach Procedure

1. Types of data breaches

1.1. A data breach occurs when any data (whether in digital or hard copy) held by UNSW is lost or subjected to unauthorised access (both internal and external to UNSW), modification, disclosure, or other misuse or interference. Examples include:

- unauthorised access to, or the unauthorised collection, use, or disclosure of, data
- accidental loss, unauthorised access, or theft of classified material, data or equipment on which such data is stored (such as loss of paper records, laptop, iPad or USB stick)
- unauthorised use, access to, or modification of data or information systems (such as, sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of confidential information (such as an email sent to an incorrect recipient or document posted to an incorrect address or addressee) or personal information posted on the website without consent
- a compromised user account (such as accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to UNSW information or information systems
- equipment failure, malware infection or disruption to or denial of IT services resulting in a data breach
- the loss or theft of a device containing personal information or health information
- a UNSW database or information repository containing personal or health information being subject to a cyber-attack
- a device, database or information repository containing personal or health information being accessed without authorisation
- UNSW inadvertently providing personal or health information to an unauthorised person or entity.

2. Data breaches involving personal information and/or health information

2.1. A data breach involving personal information and/or health information (whether in digital or hard copy) occurs when there is:

- unauthorised access to or unauthorised disclosure (whether internal or external to UNSW) of personal information or health information held by UNSW; or
- a loss of personal information or health information held by UNSW in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

2.2. Where a data breach involves personal information or health information, and a reasonable person would conclude that the access or disclosure of the information is likely to result in serious harm to an individual to whom the information relates, such a data breach will constitute an "eligible data breach" and be subject to mandatory data breach notification obligations prescribed by the Privacy and Personal Information Protection Act 1998 (NSW) (‘PIPP Act’) (and in certain circumstances by other privacy laws).
3. **Identifying and reporting data breaches**

3.1. An employee who has identified a suspected or confirmed a data breach must immediately raise a ticket via the IT Service Centre: (itservicecentre@unsw.edu.au).

3.2. On receiving the notification, the IT Service Centre will forward the notification to the Cyber Security Incident Response Team who will assess the breach to determine whether the breach constitutes a cyber security incident.

3.3. After this assessment, the Cyber Security Incident Response Team will immediately notify the Information Governance and Assurance Office about the suspected or confirmed data breach and the outcome of their assessment.

4. **Data Breach Management Committee triage**

4.1. Where a ticket is raised to report a suspected or confirmed data breach the IT Service Centre will immediately notify all members of the Data Breach Management Committee (DBM committee).

4.2. Upon such notification, the DBM committee will:
   a. immediately update the IT ticket to note that the breach has been referred to them
   b. in consultation with the Committee as a whole, assign a member of the Committee (the lead investigator) to assess and manage the data breach in accordance with the Data Breach Management Plan, set out in Appendix 2: Information Governance Instruction Manual
   c. notify the Critical Incident Team if the data breach is determined by the Committee to amount to a major data breach; and
   d. provide support and guidance to the staff member who identified the data breach.

5. **Privacy data breach**

5.1. Where the suspected or confirmed data breach involves personal information or health information, UNSW Legal & Compliance will assess the breach. If there are reasonable grounds to suspect that the breach is an eligible data breach, UNSW Legal & Compliance will:
   a. immediately update the IT ticket to note that the breach has been referred to them
   b. notify the General Counsel of the potential eligible data breach
   c. assign a lead investigator on behalf of the DBM committee and assess and manage the data breach in accordance with the Data Breach Management Plan, the mandatory data breach notification obligations prescribed by the PPIP Act, and any contractual obligations relating to the data impacted by the breach.
   d. In accordance with s 59ZJ of the PPIP Act, the functions of the Vice-Chancellor, acting as the head of UNSW for the purpose of Part 6A of the PPIP Act, are delegated to the General Counsel.

5.2. In accordance with the requirements of the PPIP Act:

5.3. If the General Counsel is satisfied that an assessment cannot reasonably be conducted within 30 days, they may approve an extension of the period to conduct the assessment. The extension may be approved for an amount of time reasonably required for the assessment to be conducted.
   a. If the extension is approved, the General Counsel must, within the 30-day period, request the Privacy Officer to start the assessment; and give written notice to the Privacy Commissioner that the assessment has commenced and that an extension for the period of the assessment has been approved.
   b. If the assessment is not conducted within the extension period, the General Counsel must, before the end of the extension period, give written notice to the Privacy Commissioner that the
6. Data Breach Management Plan

6.1. Upon referral of a suspected or confirmed data breach or eligible data breach, the lead investigator will enact the Data Breach Management Plan, as set out in the Information Governance Instruction Manual, as follows:

- immediately contain the breach and conduct a preliminary assessment
- evaluate the risks associated with the breach
- notify affected individuals or entities
- notify employee who reported the breach
- investigate the cause of the breach to prevent future breaches

7. Roles and Responsibilities

7.1. IT Service Centre

IT Service Centre receives the first notification of the suspected or confirmed data breach and creates a ticket.

7.2. Cyber Security Incident Response Team

The Cyber Security Incident Response Team assesses the suspected or confirmed data breach to determine whether it constitutes a cyber security incident.

7.3. Information Governance and Assurance Office

The Information Governance and Assurance Office sends the suspected or confirmed breach to the Data Breach Management Committee.

7.4. Data Breach Management Committee

The Data Breach Management Committee implements the Data Breach Management Plan for a suspected or confirmed data breach or eligible data breach, appoints lead investigator, notifies General Counsel of suspected or confirmed eligible data breach.

Membership of the Data Breach Management Committee includes:

- Chief Data & Insights Officer (UNSW Planning & Performance)
- Director of Cyber Security (UNSW IT, Chief Information Security Officer)
- Head of Compliance and Privacy Law (Legal)
- Privacy Officer (Legal)
- Director, Customer Services Delivery (UNSW IT)

The Data Breach Management Committee has authority to change the:

- Data breach procedure
- Information Governance Instruction Manual

7.5. Lead Investigator

The Lead Investigator investigates the suspected or confirmed data breach or eligible data breach in accordance with the Data Breach Management Plan.
7.6. General Counsel

The General Counsel, in the case of an eligible data breach notifies the Privacy Commissioner and individuals that are affected by the breach.

Effective: [XX Month] 2024   Responsible: xxxxx   Lead: xxxxx
Section 5: Use of Information Resources and Digital Communications Platforms Procedure

1. User responsibilities

1.1. UNSW information resources and provisioned digital communication platforms/technologies must be used in an ethical, lawful and responsible manner.

1.2. Users are accountable for all activities originating from their own and other UNSW accounts they access.

1.3. Users must take all reasonable steps to protect UNSW information resources from physical or digital theft, damage or unauthorised use.

1.4. Users must only store, process or transmit digital information in accordance with this policy.

1.5. Senders, recipients and managers of digital communication platforms/technologies are required to exercise due diligence to ensure the protection of confidential communications.

1.6. Digital communication platforms/technologies should not be used to send sensitive and confidential information unless the appropriate security measures including encryption have been taken.

1.7. Employees are responsible for capturing and retaining digital communications relating to UNSW's business activities so that they are accessible as records to meet business and evidential needs.

1.8. Employees are responsible for:
   a. reporting any spam, phishing, malware and other malicious digital communications
   b. reporting any digital communications sent intentionally or unintentionally that violates the Cyber Security Standard – Data Security or may result in a data breach.

2. Prohibitions

2.1. UNSW recognises that the nature of work, study and research at UNSW means that a user may use UNSW information resources and digital communication platforms/technologies for a broad range of legitimate purposes (consistent with the principles of academic freedom). However, users must not use UNSW information resources or digital communications platforms/technologies to:
   a. harass, stalk, menace, defame, vilify, or unlawfully discriminate against another person
   b. collect, use or disclose personal information except in accordance with this policy
   c. copy, download, store or transmit material which infringes the intellectual property of any other party
   d. intentionally distribute spam, phishing, chain letters, or any other type of unauthorised widespread distribution of unsolicited digital communications in contravention of the Spam Act 2003 (Cth)
e. represent or create the impression of representing UNSW unless authorised to do so
f. represent another person or claim to represent another person unless explicitly authorised, or
g. otherwise cause loss or harm to the reputation of UNSW.

2.2. Users must not:

a. use another person’s account including those assigned to other individuals and system accounts, without a delegation and approval to do so
b. share their password or other authentication factor with any other person
c. assist or permit the use of UNSW information resources or digital communications platforms/technologies by an unauthorised person
d. attempt to gain unauthorised access to UNSW information resources or digital communications platforms/technologies
e. use UNSW information resources, or personal devices, or digital communications platforms/technologies to maliciously compromise the confidentiality, integrity, availability or privacy of UNSW information resources or digital information
f. use UNSW information resources or digital communications platforms/technologies to access, display, store, copy, process, transmit or provide prohibited or restricted material, other than in accordance with section 3 of this procedure below
g. intentionally distribute spam, phishing, chain letters, or any other type of unauthorised widespread distribution of unsolicited digital communications
h. intentionally distribute viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature, including using a platform/technology to distribute software that covertly gathers or transmits information about an individual
i. use language that is excessively violent, incites violence, threatens violence, or contains harassing content
j. create a risk to a person’s safety or health, create a risk to public safety or health, compromise national security, or interfere with an investigation by law enforcement
k. attempt to manipulate, circumvent or interfere with the security and functionality of the platform/technology in any manner
l. intentionally circumvent identity controls or other cyber security controls for a malicious purpose
m. test, bypass, deactivate or modify the function of any cyber security control (including an operating system), knowingly install or use malicious software or connect an end-of-life, end-of-support, or intentionally compromised device to UNSW information resources or digital communications platforms/technologies except for research or teaching purposes; or (ii) with written approval of the Head of School or equivalent and in an isolated testing environment or isolated network
n. collect or use email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting).
o. spidering and harvesting data from UNSW websites by the UNSW community.

3. Prohibited and restricted material

3.1. Users can access, display, store, copy, or transmit prohibited or restricted material on or using UNSW information resources for research or teaching purposes only (i) in accordance with all laws,
policies, procedures, and standards, including the Australian Code for the Responsible Conduct of Research; and (ii) with human or animal ethics approval where appropriate; and (iii) with the express written approval of a relevant Deputy Vice-Chancellor (for prohibited material) or a Head of School or equivalent (for restricted material).

3.2. Users can access, display, store, copy, or transmit prohibited or restricted material on or using UNSW information resources for the purpose or intention of investigation of a potential breach of a code of conduct, policy, procedure by the Conduct and Integrity Office or Human Resources.

4. Personal use

4.1. UNSW provides access to UNSW information resources and digital communications platforms/technologies for users to perform work, research or studies at UNSW and all usage must be consistent with that purpose, other than the exceptions in the next clause.

4.2. Users are permitted limited and incidental personal use of UNSW information resources and digital communications platforms/technologies. However, this use must not:

a. directly or indirectly impose an unreasonable burden on any UNSW information resource or burden UNSW with incremental costs
b. unreasonably deny any other user access to any UNSW information resource
c. contravene any law, UNSW’s Code of Conduct and Values and UNSW policies or interfere with or conflict with UNSW’s functions.
d. in the case of employees, interfere with the execution of their responsibilities.

4.3. Users who store, process or transmit their own personal information as part of their personal use of a UNSW information resource are responsible for deciding how that information is secured (such as, encrypted) and backed up.

4.4. UNSW is not responsible for ensuring that personal data is retained or providing such data to a user.

4.5. Personal emails remain subject to the provisions of this policy and as such may be accessed in accordance with the monitoring and surveillance section of this procedure below.

4.6. Excessive use of UNSW information resources (such as to generate or mine crypto currency) is not permitted, except for research or teaching purposes, and with the express written approval of the Head of School or equivalent.

4.7. Employees and students must not use UNSW information resources or digital communications platforms/technologies for:

a. financial or commercial gain for themselves or any third party; or
b. private professional practice.

5. Personal devices

5.1. Employees performing duties at UNSW using personal devices must ensure that these devices:

a. are password protected, or have an equivalent access restriction mechanism enabled
b. have malware protection enabled, where available
c. are patched or updated promptly and
d. are encrypted.

5.2. Employees must report the loss or theft of, or damage of a personal device containing UNSW data to UNSW Campus Security and to the IT Service Centre at the earliest opportunity in accordance with the reporting data breach requirement set out in the Data Breach Procedure.
5.3. UNSW does not guarantee that a personal device will be able to access, or be compatible with, all UNSW information resources.

6. Terms of use

6.1. UNSW takes reasonable precautions to protect the security of UNSW information resources and digital communications platforms/technologies but does not guarantee that UNSW information resources and digital communications platforms/technologies will always be available, secure, confidential, or free from defects, including malicious software.

6.2. UNSW accepts no responsibility for loss or damage (including consequential loss or damage or loss of data) arising from the use of UNSW information resources and digital communications platforms/technologies, or from the maintenance and protection of UNSW information resources and digital communications platforms/technologies.

6.3. UNSW may take any necessary action in accordance with the Cyber Security Standard – Data Security, to mitigate any threat to UNSW information resources and digital communications platforms/technologies, with or without notice.

6.4. UNSW reserves the right to:

a. limit or terminate the use of UNSW information resources and digital communications platforms/technologies, with or without notice

b. view, copy, disclose or delete digital information stored, processed, or transmitted using UNSW information resources and digital communications platforms/technologies

c. monitor or examine the security of any device connecting to UNSW information resources and digital communications platforms/technologies, to identify or address a cyber security threat

d. monitor, access, examine, take custody of, and retain any UNSW information resource and digital communications platforms/technologies.

6.5. Access to a UNSW information resource, or storage, processing and transmitting of data (including email) may be delayed or prevented in the event of misuse or suspected misuse, or in the event of a security event or suspected security event.

7. Mailing lists and broadcasts

7.1. Transmission of digital communications to multiple users must only be undertaken using a UNSW approved service provider.

7.2. The transmission must be controlled so that users do not receive a large quantity of unwanted and unsolicited digital communications as this can reduce the effectiveness of the digital communications platforms/technologies.

7.3. Users may solicit communications on a particular topic by subscribing to a UNSW mailing list or third-party mailing list from which they can also unsubscribe at will.

7.4. Unsolicited communications may only be sent to multiple users where the communication is related to their UNSW duties and the sender has a relevant work relationship with the recipients.

7.5. Broadcast communication e.g. email to students should be conducted via Student Communications.

7.6. Special interest groups must issue invitations to join before including any group or individual in a mailing list, and members have the right to unsubscribe at will.

7.7. Users who wish to send a broadcast digital communication to the UNSW community, or a substantial subset of the community (such as all academics) must follow the procedure set out in Appendix 2: Information Governance Instruction Manual.
8. Scanned, electronic and digital signatures

8.1. The use of scanned signatures is discouraged as they are vulnerable to forgery. Alternate solutions such as electronic and digital signatures should be used instead for all official documents.

9. Retention of digital communications

9.1. Digital communications sent and received by employees acting in the course of their duties form part of UNSW’s official records.

9.2. The record and information management procedures set out above also apply to digital communications.

10. Terminating access

10.1. UNSW may terminate the access of any user whom it believes is not operating in compliance with this procedure or the law.

11. Monitoring and surveillance

11.1. All data stored, processed, or transmitted using any UNSW information resource and digital communications platforms/technologies

a. may be recorded and monitored on an ongoing and continuous basis, in accordance with the UNSW Cyber Security Standards

b. may be subject to the Government Information (Public Access) Act 2009 (NSW)

c. may be subject to the Privacy and Personal Information Protection Act 1998 (NSW)

d. may be subject to the Health Records and Information Privacy Act 2002 (NSW)

e. may be subject to the State Records Act 1998 (NSW), and

f. will remain in the custody and control of UNSW other than where the conditions for external sharing of UNSW data stated in the data management procedure section above are met.

11.2. Users should be aware that personal use of UNSW information resources and digital communications platforms/technologies may result in UNSW holding personal information about the user or others which may be accessed and used by UNSW to ensure compliance with this and other policies.

11.3. Scanning and monitoring of personal drives and devices connected to a UNSW Information Asset must not unreasonably intrude into the personal affairs of individual employees or students.

11.4. The following approvals are required for access by a person other than the owner or custodian to UNSW storage services and storage devices such as mailboxes, Microsoft 365 services, hard drives, and file shares that may also contain personal information.

<table>
<thead>
<tr>
<th>Circumstance</th>
<th>Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>When required for legal proceedings or as required by law (such as to comply with a notice to produce or subpoena).</td>
<td>General Counsel and any one of: Chief People Officer, Director, Conduct &amp; Integrity, Chief Information Officer.</td>
</tr>
<tr>
<td>For cyber security purposes</td>
<td>Chief Information Officer; or Director, Cyber Security and any one of: General Counsel, Chief People Officer, Director, Conduct &amp; Integrity</td>
</tr>
</tbody>
</table>
11.5. No access is to be provided without two signatures. An authorisation from only one person (regardless of the seniority of the person or the role that they perform) is insufficient to provide access.

11.6. UNSW IT will:

   a. provide a University-wide directory, which will include email addresses
   b. make available a mailing list system for creating email lists and to establish lists for valid purposes
   c. monitor the performance of the existing central email system and its usage to ensure the service meets the needs of its users within the available resources
   d. administer usage of the central service and apply temporary or permanent usage constraints or limits to the service for any user (including discontinuance or deactivation) who is in breach of this policy or any other UNSW rules or policies, or applicable Federal or State law. Any such decision may be appealed to the Chief Information Officer.
   e. retroactively detect and remove malicious emails that have already been delivered to users.

11.7. UNSW may exercise its legal right to read any digital communication sent via UNSW information resources. The information viewed by any third party authorised to read the digital communication (i.e. other than the sender or recipient), will only be used for the sanctioned purpose.

12. Identity management

12.1. The use and disclosure of an individual’s digital identity must comply with this policy, UNSW’s Privacy Management Plan and Privacy Statements.

12.2. Forms of identity used to access UNSW information resources should not be published together with the identity of the user. However, identities may be published within UNSW’s internal directory.

12.3. The identity of students can be displayed in a teaching context, to an individual student or between an individual student and their teacher or class support. However, employees and students must not:

   a. display a list of students’ identities to a class or other group, and/or
b. share a list of students’ identities to a class or other group without an approved data sharing approval.

12.4. UNSW Estate Management and other UNSW business units may provide user’s identities with access to physical buildings and to spaces within buildings. An identity for this purpose should be classified as private under the UNSW Data Classification Standard.

12.5. A list of persons who have access to spaces which includes first name, last name and identity can be shared with employees who have legitimate business reasons to have access to this information. This information must not be shared via email.

13. Misuse

13.1. In the event of misuse or suspected misuse of UNSW information resources UNSW may:

a. withdraw or restrict a user's access to UNSW information resources
b. commence disciplinary action
c. notify the Police or other relevant government authority.

14. Reporting events

14.1. The loss, theft or damage to UNSW information resources must be reported at the earliest opportunity to UNSW Campus Security and to the IT Service Centre in accordance with the reporting data breach requirement set out in the Data Breach Procedure.

14.2. Any person who notices a potential or actual cyber security incident must report it as soon as possible to the UNSW IT Service Centre or UNSW IT Cyber Security Team.

15. Non-compliance

15.1. Any non-compliance with the use of Information Resources and digital communications platforms/technologies procedure must be approved in accordance with the Cyber Security Standard - Framework Exemption, including a mandatory risk assessment and agreed compensating controls.

16. Roles and Responsibilities

16.1. The Chief Information Officer

See the responsibilities section of the Information Governance policy above for the responsibilities and authorities of the Chief Information Officer.

16.2. UNSW IT

UNSW IT facilities, services and manages UNSW information resources.

16.3. Users of UNSW information resources and digital communication platforms/technologies

Users of UNSW information resources are responsible for using UNSW information resources in accordance with this policy.

Effective: [XX Month] 2024  Responsible: xxxxx  Lead: xxxxx
Section 6: Use of Artificial Intelligence Systems or Tools Procedure

1. User responsibilities

1.1. Users are accountable for all activities originating from their use of artificial intelligence (AI) systems or tools.

1.2. AI systems or tools must be used ethically, lawfully and responsibly.

1.3. Users of AI systems or tools must ensure that confidentiality is maintained throughout the data management life cycle.

2. AI self-assurance assessment

2.1. Before any AI system or tool is used an AI self-assurance assessment must be conducted.

2.2. The AI self-assurance assessment (based on the New South Wales Government’s AI Assurance Framework) comprises the following elements that must be considered before using an AI system or tool:

   a. sensitive data - The AI system or tool does not involve the use or creation of highly sensitive, sensitive, commercial and/or personal data without consent/approval

   b. harm - The AI system or tool is respectful of fundamental human rights, the rights of the child and/or the environment

   c. compliance - The AI system or tool complies with UNSW policies, relevant legislation, and the Ethical and Responsible Use of Artificial Intelligence at UNSW principles

   d. fairness - The outputs of the AI system or tool are equitable, inclusive, accessible and free from bias and there is a mechanism for challenging outcomes

   e. business value - The AI system or tool aligns with UNSW’s core values, Strategic Plan, improves services or efficiencies and there is an approved budget for the initial and ongoing costs

   f. transparency and accountability - The AI system or tool provides identifiable, explainable, reliable, and interpretable outputs to the user and there is clear accountability and monitoring to ensure that the system or tool continues to function as designed.

2.3. Data used to train the AI system or tool must be diverse and representative of the population it serves.

2.4. Data must only be used and stored in an AI system or tool in accordance with its classification.

2.5. AI systems and tools must be continuously monitored by users after deployment to identify any emerging biases or unfair outcomes.

3. Roles and Responsibilities

The Chief Information Officer
See the responsibilities section of the Information Governance policy above for the responsibilities and authorities of the Chief Information Officer.

Director of AI Strategy Education, DVCESE

The Director of AI Strategy Education is responsible for coordinating UNSW’s response to generative AI and leading the development of UNSW’s AI Education Action Plan.

Users of AI systems or tools

Users are responsible for using AI systems or tools in accordance with this policy.

Effective: [XX Month] 2024  Responsible: xxxxx  Lead: xxxxx
Appendix 1

Legislative compliance

This policy is intended to ensure that UNSW complies with the:

1. State Records Act 1998 (NSW)
2. Evidence Act 1995 (NSW)
3. Privacy Act 1988 (Cth)
5. Health Records and Information Privacy Act 2002 (NSW)
6. Privacy and Personal Information Protection Act 1998 (NSW)
7. Children and Young Persons (Care and Protection) Act 1998 (NSW)
8. Public Finance and Audit Act, 1983 (NSW)
9. University of New South Wales Act 1989 (NSW)
10. Work Health and Safety Act 2011 (Cth)
12. Copyright Act 1968 (Cth)
13. EU General Data Protection Regulation 2016/679
15. Workplace Surveillance Act 2005 (NSW)

Supporting documents

- Information governance instruction manual (internal access only)