HSU HEALTH SCIENCES UNIVERSITY

Version: 2.0
Effective from: September 2025
Policy Owner: Head of Research
Category: Research

Research Data Management Policy and Procedures

Purpose

In accord with the HSU Research & Knowledge Exchange Strategy, this policy provides part of the supporting framework to deliver Health Sciences University's (HSU) commitment to ensuring that those involved in research activities are well-informed and compliant with current legal, regulatory, and institutional principles and expectations when planning, conducting, and disseminating their work. HSU recognises that research data is a valuable institutional asset, and the role of robust research data management in underpinning institutional strategic development, essential functions, and research integrity.

Good practice in research data management enables HSU and its researchers to meet the standards and responsibilities set out in the HSU Code of Good Research Practice and to meet funder, ethical, legal and other responsibilities. It is also essential for enabling and safeguarding the longevity and continuing intelligibility of research data. The policy sets out the support and guidance that researchers should follow to enable them to promote good practice in research data management, to foster responsibility for data management, and to ensure the sharing of eligible research data with as few restrictions as possible, while at the same time respecting concerns in relation to privacy, safety, security and commercial interests.

This policy applies to HSU staff, postgraduate research students and those associated with the university such as visiting fellows and visiting professors (henceforth referred to as 'researchers'). All researchers must adhere to their obligations under this Policy. The policy does not normally apply to taught postgraduate and undergraduate students, except in exceptional circumstances, including, but not limited to, where research findings are included in published research outputs.

As part of a commitment to research excellence, HSU seeks to promote the highest standards in the management of research data throughout the research data lifecycle. As such, research data will be managed in accordance with this and with the University's other policies and guidelines including:

- Code of Good Research Practice
- Research Ethics Policy & Procedures
- Data Protection Policy
- Privacy Notice – Research Participants
- Publications & Open Access Policy & Procedures
- Research Misconduct Policy & Procedures
- Research Data Sharing Agreement [*due to be published in autumn 2025*]
- IT Acceptable Use Policy
- Data Protection Breach Policy

Guidance and support for research data management is available from the HSU RKE Hub: https://aeccacuk.sharepoint.com/sites/Researchknowledgeexchange/SitePages/Research-Data-Management.aspx. The deliberate or reckless mismanagement of research data and/or primary materials constitutes unacceptable research conduct and should be reported in line with HSU's Research Misconduct Policy & Procedures.

The Research Team (research@aecc.ac.uk) can help with queries about research data management. In addition, the Data Protection Officer (dpo@aecc.ac.uk) can be contacted with questions at any time around data protection and storage.

Regulatory Context

The management of research data at HSU is shaped by a combination of legal requirements, funder mandates, and institutional policies that reflect national and international standards for research integrity, data protection, and open scholarship.

HSU embraces the international drive towards open science and is committed to developing a research culture that facilitates the advancement and dissemination of knowledge for the public good. Recognising that data

from HSU research can be a public good, produced in the public interest and for societal benefit, HSU embraces the Concordat on Open Research Data and the UKRI Common Principles on Research Data. Making HSU research data freely accessible, wherever this is appropriate, ensures that a wide range of audiences can freely discover, engage, and reuse its research. This is beneficial to our researchers, HSU as an institution, academia, and society.

Key regulatory and policy considerations include:

- UK Data Protection Law: All research involving personal data must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Researchers must ensure that personal data is collected, processed, stored, and shared lawfully, with due regard for privacy, consent, and data minimisation.

- Research ethics and integrity: Research conducted at HSU must follow the principles set out by bodies such as UK Research and Innovation (UKRI), the Universities UK Concordat to Support Research Integrity, and relevant professional or disciplinary codes of ethics. Ethics review is required for studies involving human participants, personal data, or other sensitive contexts, as set out in the HSU Research Ethics Policy and Procedures.

- Funder requirements: UK research funders, including UKRI, the Wellcome Trust, and NIHR, require researchers to develop and follow data management plans (DMPs), and to make research data as open as possible, as closed as necessary. Compliance with these requirements is a condition of funding.

- Intellectual Property (IP) and copyright: Research data may be subject to IP rights and licensing considerations. Researchers must be aware of any contractual or legal restrictions on data sharing, including third-party data use agreements or collaborations with industry partners.

- Freedom of Information (FOI) and Open Research: As a public institution, HSU is subject to the Freedom of Information Act 2000, which may apply to research data in some circumstances. The university also supports the principles of open research, encouraging data sharing and reuse, in line with ethical and legal obligations.

By understanding and applying this regulatory context, researchers at HSU can ensure that data is managed responsibly, supports reproducible research, and complies with relevant legal and funder expectations.

Definitions

Research data: All researchers create some type of data as part of the research data lifecycle. Research data refers to the recorded information (regardless of the form or the media in which it may exist) necessary to support or validate a research project's observations, findings or outputs. Along with research publications, research data forms an important part of the scholarly record.

Data management plan (DMP): A formal document that outlines how research data will be handled throughout the research lifecycle. It describes how data will be collected, documented, stored, protected, shared, and preserved, both during the project and after it is completed. A DMP ensures that data is managed in accordance with legal, ethical, and funder requirements, and supports transparency, reproducibility, and long-term accessibility.

Research lifecycle: The sequence of stages through which a research project progresses—from planning and data collection, to analysis, publication, preservation, and sharing.

Personal data*:* Information relating to an identifiable living individual, as defined under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Sensitive data*:* Data that must be protected due to ethical, legal, or contractual obligations, such as data involving human participants, health records, or commercially sensitive information.

Metadata: Descriptive information about a dataset that helps others understand, find, and reuse it. Metadata may include details about the creator, date of collection, methodology, format, and access conditions.

***FAIR principles**:* A set of guiding principles to make data Findable, Accessible, Interoperable, and Reusable – promoting good data stewardship and enabling reuse by others.

***Open research / open data**:* The practice of making research outputs, including data, openly available to maximise transparency, reproducibility, and impact, subject to legal, ethical, or commercial constraints.

Archiving / preservation: The long-term storage and maintenance of research data to ensure its continued availability and integrity after the conclusion of a project.

Key Responsibilities

The **Head of Research** is the owner of this policy.

The **Research & Innovation Committee** is responsible for endorsing the policy. The **Academic Board** is responsible for approving the policy.

Researchers are responsible for:

General:

- Principal Investigators and project leads have overall responsibility for effective data management during research projects. However, all researchers have a personal responsibility to effectively manage the research data generated within or obtained from their research and must act in accordance with this policy.

- Responsibility for ensuring the effective day-to-day management of research data lies with the researcher. This includes understanding and complying with any provisions regarding the ownership, preservation and dissemination of research data of research contracts with or grants to the University.

Data management plans:

- In line with good practice, researchers are strongly encouraged to routinely prepare, maintain, and adhere to a data management plan for their research projects. Data management plans should address the capture, management, integrity, confidentiality, retention, ownership, sharing and publication of research data, including compliance with relevant legal and ethical frameworks. Plans must also adhere to any funder requirements where these exist. Links to guidance and examples of data management plans are available on the RKE Hub.

Externally funded and collaborative research:

- Researchers will identify the resources required to effectively manage research data and will seek, where possible, to recover the direct costs of managing research data and any work needed to make the data available for sharing from their research funder. This is particularly relevant where research data management plans identify additional costs such as extra storage, long-term retention, or significant data management effort.

- Where research is conducted in collaboration with external research partners, researchers must ensure that suitable agreements for the ownership and use of research data are prepared and agreed in writing by the parties concerned before the project starts. This should also cover the rights and responsibilities of each party regarding how the data will be collected, including key decisions about data storage, backup and security, registration, access, transfer, retention, destruction or archiving, and licensing. Help, guidance and template agreements are available from the Research Team.

Data collection, processing and analysis:

- Researchers must be aware of their and the University's legal obligations and potential liability when processing data relating to people to ensure compliance with handling data protected by the UK Data Protection Act (2018) and the European Union General Data Protection Regulation (2016), together with any other applicable data protection or privacy laws). Researchers will protect confidential, personal, and sensitive research data in accordance with legal and ethical requirements related to the research they conduct. Legal, ethical and commercial constraints on the sharing of research data must be considered at the initiation of the research process and throughout the research data lifecycle and will normally be described in a data management plan.

Data loss or security breach procedure:

- There are potentially significant repercussions for the University and the individuals affected arising from a data loss or security breach. Where this occurs or you suspect it may have occurred, you must follow the guidance provided in the University's Data Protection Breach Policy:
    - It is important that this is done immediately, as it may be possible to reduce the impact of the breach by remote deletion, removal or other means.
    - Follow their guidance on dealing with the security breach and keep the Data Protection Officer up to date with any further information about it that you become aware of.
    - Do not approach any individual data subjects, suppliers, regulators or make any public announcements about the security breach incident without the prior agreement of the Data Protection Officer.

Data storage, access and sharing:

- Researchers must ensure that all research data in digital and computer-readable form:
    - is stored securely in a durable format appropriate for the type of research data in question;
    - is stored with adequate metadata and/or documentation to facilitate identification and support effective reuse of research data where this is appropriate;
    - is backed-up regularly in accordance with best practice in the relevant field of research.

- Researchers must ensure that all non-digital research data that is unsuitable for digitisation, but which is significant should be (see clause 5.4 for a definition of non-significant research data):
    - stored securely;
    - labelled, indexed or categorised appropriately to identify the research data in question and support effective reuse of research data where this is appropriate.

- Before sharing research data during or after a project, researchers must determine whether this is permissible considering data sharing restrictions, intellectual property rights (IPR) ownership, ethical, privacy, confidentiality requirements or any legal, regulatory or funding restrictions. In addition, researchers must consider whether research data has commercial potential and in consultation with the Research Team consider if it is suitable for IP protection and/or transfer.

- If it is deemed appropriate to share the research data, researchers should offer the research data they have selected for preservation and sharing to an appropriate data repository, along with sufficient descriptive metadata and documentation to ensure that it can be found and understood. HSU does not yet have an institution repository for research data. However, external data repositories are available (the Research Team can advise on this and information is available on the RKE Hub). Also, if the research is a collaboration with another university, the other university may have an institutional data repository to which the data could be uploaded.

- Researchers must include a data access statement in their published research outputs which clearly describes how and on what terms any supporting data may be accessed. See Section 3.1 of the HSU Publications & Open Access Policy & Procedures for guidance.

- Researchers are encouraged to obtain an ORCID identifier to help them record and report their work. This identifier can be used in publications, grant applications, funder reporting and impact tracking.

- Technicians, professional, and support staff instrumental in contributing to the collection and/or generation of research data should be acknowledged, and their contribution specified in descriptive metadata and in data access statements.

Data disposal:

- Researchers must securely dispose of research data identified for deletion or destruction, in accordance with legal, ethical, research funder and collaborator requirements and with particular concern for the confidentiality and security of the data. The agreed processes for the timing, manner and recording of research data disposal and destruction should be included in the research data management plan and stored with other project information and documentation. Data disposal must be carried out in accordance with HSU's Data Protection Policy.

Postgraduate research students: The University believes that embedding research data management practice in early career researchers is critical to establishing an effective data management ethos. Therefore,

where research is undertaken by postgraduate researchers, it is the responsibility of the staff member supervising their project to ensure that the postgraduate researcher has a clear understanding of their research data management responsibilities and engages with training and development as necessary. Supervisors should work with the postgraduate researcher to determine which research data is selected for archiving and sharing and to decide an appropriate route to achieve this. All postgraduate researchers should produce and maintain a research data management plan.

Managers of researchers (e.g. Heads of School, School Research Leads and other staff responsible for research staff and students) are responsible for promoting good practice in all aspects of research governance and integrity including research data management. They should ensure that staff and students are aware of this policy and their responsibilities and obligations in effective management of research data. They should also identify or promote training where gaps in these skills are identified.

Heads of School/equivalent assume stewardship of data once the researchers involved in compiling the data leave HSU. They must work with the researcher to agree how research data will be located and how it will be stored. This role may be delegated to a dedicated data steward or stewards to act as custodian of such data on HSU's behalf until it is destroyed.

HSU acknowledges its obligations under research funders' data policies and codes of practice to ensure that sound systems are in place to promote and reinforce good practice in research data management. HSU is committed to providing:

- researchers with access to training, support, advice and information on all aspects of research data management;
- guidance on accessing services and facilities for the storage, backup, registration, deposit and discovery of research data;
- the necessary resources to enable the provision of these services, facilities and training.

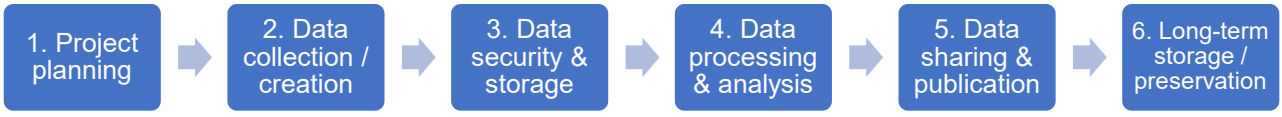
Policy principles

The policy aims to ensure that research data is:

- Stored securely and safely, with appropriate measures in place to protect against loss, damage, or unauthorised access;
- Identifiable, retrievable, and accessible when required, subject to appropriate permissions and ethical considerations;
- Accurate, complete, authentic, reliable, and coherent, providing a faithful representation of the materials generated or collected during the research process;
- Managed in compliance with legal, ethical, and contractual obligations, including UK data protection laws, university policies, and where applicable, the requirements of funding bodies;
- Made available for reuse where appropriate, in line with ethical considerations, data sharing agreements, and the principles of FAIR (Findable, Accessible, Interoperable, and Reusable) and open access.

PROCEDURES

Research Data Management Flowchart



This flowchart should be followed alongside the Responsibilities section above.

Step 1: Project planning:

- Identify types of data to be collected/generated
- Assess legal, ethical, and funder requirements
- Draft a Data Management Plan (DMP)
- Plan for secure storage, backup, and sharing
- Seek ethics approval (if required)

Step 2: Data collection / creation:

- Collect or generate data using agreed protocols
- Record metadata and documentation
- Ensure data quality and version control
- Apply appropriate consent and licensing (if needed)

Step 3: Data storage and security

- Store data securely (e.g., university servers, encrypted storage)
- Back up data regularly
- Restrict access to sensitive/personal data
- Maintain documentation and file organisation

Step 4: Data processing and analysis

- Use approved software/tools
- Maintain records of processing steps
- Anonymise or pseudonymise personal data if required
- Continue to update metadata

Step 5: Data sharing and publication

- Determine what data can be shared (and under what conditions)
- Choose a suitable repository (e.g. Zenodo, UK Data Service)
- Apply appropriate licences (e.g. CC BY, CC0)
- Ensure data cited and linked in publications

Step 6: Long-term storage / preservation

- Deposit final dataset and metadata in a trusted repository
- Follow retention and disposal schedules
- Ensure data remains accessible and usable (FAIR principles)
- Close out DMP if required by funder

Information Management requirements

Definitive documentation relating to the policy is held by the Research Team.

Researchers at HSU are expected to manage research data responsibly and in accordance with legal, ethical, funder, and institutional requirements. The following information management practices must be followed throughout the research lifecycle:

1. Data storage and security
    - Research data must be stored on secure and approved storage platforms (e.g. university-managed servers, secure cloud services).
    - Access to data must be appropriately restricted based on sensitivity, using permissions and access controls.
    - Personal and sensitive data must be encrypted in storage and during transmission.
    - Regular backups must be made using automated or institutionally recommended systems to prevent data loss.

2. Data organisation and documentation
    - Data should be organised using consistent, meaningful file naming and folder structures.
    - Sufficient metadata and documentation must be created and maintained to enable understanding, validation, and reuse of the data by others (or by the researcher in future).
    - Version control practices should be applied to track changes and maintain data integrity.

3. Access and collaboration
    - Data access should be limited to those with a legitimate need, and access controls should be reviewed regularly.
    - Where collaboration is involved, data sharing agreements or memoranda of understanding should be in place to govern data access, usage, and ownership.
    - Any external storage solutions (e.g. third-party cloud services) must comply with university policies and UK data protection laws.

4. Data retention and disposal
- Data should be retained for the period specified by funders, legal requirements, or university policy (a minimum of 10 years after project completion, see Data Retention Periods section).
- Sensitive or personal data must be securely deleted when no longer needed, using approved disposal methods (e.g. secure deletion tools).
- Disposal must be documented where required.

5. Artificial Intelligence (AI) and data
- Researchers using AI tools for data analysis must ensure that the data used in AI models is accurate, representative, and of high quality. Any data preprocessing or manipulation by AI systems must be well-documented and transparent to support reproducibility and trustworthiness.
- AI models may introduce biases based on the data they are trained on. Researchers must take steps to identify and mitigate any potential biases in AI systems to ensure fairness, transparency, and ethical use of data.
- In cases where AI is used to generate data (e.g., synthetic datasets or models), clear documentation on the origin, methodology, and assumptions behind the AI-generated data must be provided.
- Data resulting from AI models should be treated as research data, with appropriate metadata, version control, and retention protocols.

6. Compliance and support
- Researchers must ensure compliance with relevant data protection regulations, such as UK GDPR and the Data Protection Act 2018.
- Support and guidance are available from the HSU Research Team, Library Services, IT Services, and Data Protection Officer.

Data retention periods

All research data which is stored in accordance with this policy should be held for a minimum period of 10 years from collection, creation or generation of the research data or publication of the research results (whichever is the later) provided appropriate safeguards are in place to protect any personal data necessary to achieve the research objectives contained within it.

Research data will be retained for longer than ten years:
- where an increased retention period is required to meet HSU's statutory obligations, contractual obligations or the guidelines of the body funding the relevant research project;
- where the results of the research have resulted in a patent application;
- where the results of the research become contentious or subject to challenge at any time during the initial 10-year retention period, in which case Research Data should be retained pending review and not destroyed or otherwise disposed of until the matter is fully resolved.

Research data may be retained for longer than ten years where the research has a public interest or heritage value.

Research data that is not deemed ‘significant’ data need not be retained beyond the end of the research project. Non-significant data could include early research notes, early versions of later documents, or material which is expensive to store but quick and easy to collect again. Unless a publication is planned from the research, all research data resulting from work undertaken by taught undergraduate and postgraduate students towards their dissertations would fall into this category and need not be retained after the degree has been awarded.

Reporting and Oversight requirements

To ensure compliance with this policy, HSU will implement the following:
- Data Management Plan (DMP) Review: All externally funded research projects must submit and maintain an up-to-date DMP, which will be reviewed at key stages.
- Audits and monitoring: Periodic audits may be conducted to assess compliance with RDM practices. Researchers must cooperate with these reviews and report any data management issues (e.g., data loss or breaches) immediately.
- Oversight bodies: The Research & Innovation Committee will oversee RDM policy implementation, while the Research Team will provide ongoing support and training.

- Incident reporting: Any data breaches or security incidents must be reported promptly to the Data Protection Officer (DPO) following university procedures.
- Policy review: The RDM policy will be reviewed biennially to ensure it remains compliant with legal requirements and best practices.

Good practice

In drafting this policy and procedures, good practice has been adopted from other universities including:

- University of Edinburgh: https://www.ed.ac.uk/information-services/about/policies-and-regulations/research-data-policy
- University of Northampton: https://www.northampton.ac.uk/wp-content/uploads/2021/04/research-data-management-policy.pdf
- University of Southampton: https://www.southampton.ac.uk/about/governance/regulations-policies/policies/research-data-management
- University of Surrey: https://www.surrey.ac.uk/sites/default/files/2022-06/research-data-management-policy_0.pdf
- University of York: https://www.york.ac.uk/staff/research/governance/research-policies/research-data-management-policy/
- University of Winchester: https://www.winchester.ac.uk/media/critical-documents/Research-Data-and-Records-Management-Policy.pdf

Version	2.0
Approving body	Academic Board
Policy Owner	Head of Research
Date approved	11 June 2025
Effective from	September 2025
Review date	2026/27
Target Audience	Health Sciences University staff and postgraduate research students conducting research (this includes visiting fellows/professors)
Publication	HSU Staff Resource SharePoint site
Equality analysis	This Policy has been developed with due regard to the University's general equality duty and no direct impact has been identified.