Information Governance and Records Management Policy

April 2022

POLICY

Approving authority:	University Executive
Consultation via:	Global Information Governance and Data Protection Committee, Global Operations Executive, Combined Joint Negotiation and Consultative Committee
Approval date:	19 April 2022
Effective date:	19 April 2022
Review period:	Five years from date of approval, when the University Strategy is superseded, or more frequently if required
Responsible Executive:	Secretary of the University
Responsible Office:	Information Governance, Governance and Legal Services
Territorial Scope:	Global

HERIOT-WATT UNIVERSITY
POLICY TITLE

CONTENT

1. INTRODUCTION

1.1 Effective and efficient management of the University's information assets underpins all the University's functions and activities and contributes to delivery of the University's mission and strategic priorities. Without good information management, the University cannot operate and cannot meet its obligations.

1.2 **Managing the University's information assets is a core corporate function**, like managing financial assets or health and safety risks. Everyone working on behalf of the University – wherever in the world they may be – has an important role to play, supported by expert professional advice.

1.3 Managing the information individuals create, receive, and use when working on behalf of the University is a core part of that work. This Policy makes those existing responsibilities explicit and establishes a framework of support.

1.4 This Policy affirms the University's **commitment to managing our information assets effectively** by applying information governance principles (see section 3 below) to support the University to be accountable for, and transparent about, its activities.

1.5 This Policy sets out a framework of governance and accountability for managing the University's information assets and outlines an **Information and Records Management Programme** (see section 7 below), that operates alongside the Global Privacy Programme and the Information Security Management Programme to embed effective information governance in all the University's areas of work.

1.6 This Policy has been updated to support Strategy 2025 in addition to meeting the University's obligations under the Scottish Ministers' Code of Practice on Records Management By Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 (see section 8.4 below).

1.7 Some words and phrases in this Policy have specific definitions that are provided in section 9 below. For example: Information; data; record; information asset; confidential information; information system; metadata; transitory information; vital information; information governance; records management.

1.8 Appendix 1 provides a summary of this Policy's key messages.

2. PURPOSE

2.1 The University recognises that **information is a precious University asset** and is committed to creating, maintaining, using, and managing information assets (which are defined in section 9 below) to:

- Deliver the University's mission and strategic objectives, including providing quality services, and supporting learning, teaching, and research
- Meet legal, compliance and accountability obligations, including documenting the University's decisions and principal activities and supporting good governance and decision making

POLICY

- Protect the University's corporate memory and preserve an adequate historical record

Mission and strategic objectives

2.2 The University's mission is "to create and exchange knowledge that benefits society". Data and information are fundamental building blocks for the development of knowledge. Effective management of the University's information assets is therefore essential to the University's mission.

2.3 Effective information asset management is fundamental to deliver Strategy 2025. Realisation of the goals to be a "Globally Integrated Connected University", continue "Pioneering in Education", "Excelling in Research and Enterprise" and "Building Flourishing Communities" relies on:

- Access to the same high-quality information – "Single Point of Truth" – to inform our choices, actions, and decisions, and provide accountable evidence of these
- The same effective information systems – "One Heriot-Watt Way" – to enable exchange, collaboration, and partnership
- Reliable, authentic, accurate, and trustworthy information being available to the right people at the right time, wherever they are located so our community can get straight to work (whether delivering our learning and teaching strategy, providing high-quality services to stakeholders, or leading intellectual discovery) without first overcoming information quality or availability hurdles
- Breaking down information silos – by knowing what information assets we hold and where they are – to enable innovation and synergy, inspiring our community and supporting its members to belong, collaborate, celebrate, and live our values
- High quality management information, metrics, and measures, which provide trusted, timeous analytical insights so that we can respond to fast-changing environments
- Digital transformation that is supported by quality information and effective information asset management systems and processes.

Legal, compliance and accountability obligations

2.4 The University "has no appetite for breaches of legislation, regulation, professional standards or ethics" (Risk Appetite Statement, September 2019). Meeting the University's legal and regulatory obligations relies on effective information asset management. Reliable information assets provide evidence of our rights and interests and demonstrate that we have fulfilled our legal and regulatory obligations, for example by providing evidence of fair and consistent practice. Transparent and accountable information systems help to earn the trust of our stakeholders so that they can, for example, be confident that we maintain the confidentiality of any confidential information they share with us, use their personal data lawfully and in compliance with their rights and the data protection principles.

2.5 This Policy, and supporting procedures and guidance, are required to meet the University's obligations under the Scottish Ministers' Code of Practice on Records Management By Scottish Public Authorities under the Freedom of Information

POLICY

(Scotland) Act 2002. It also supports compliance with the legal requirements set out in section 8.4 below.

Business continuity, corporate memory, and historical record

2.6 Information asset management supports risk management, business continuity and protects our corporate memory.

2.7 University business will be disrupted if information assets are lost, compromised, or if their confidentiality, availability, integrity, or resilience is damaged.

2.8 The Heriot-Watt University Museum and Archive Collections are our corporate memory. The collections record the University's unique heritage from its ground-breaking origins in 1821 as the Edinburgh School of Art, the world's first Mechanics Institute, and continue to develop to reflect our current achievements and future plans. The collections reflect the history of our campuses and the communities in which they are based and our dynamic evolution into a global University with Scottish roots.

2.9 To maintain our corporate memory, it is essential that we identify current and semi-current information assets that have archival value and will (ultimately) be transferred to the University Museum and Archive for permanent preservation. But digital information assets are vulnerable. Unlike paper, digital assets require active digital preservation early in their lifecycle if we are to be confident that they will be available for future generations.

3. OBJECTIVES

3.1 Through this Policy the University aims to be accountable for, and transparent about, its activities by applying the following **information governance principles**.

3.2 We create, receive, and maintain information assets that:

- are **Effective**
  Information assets are consistent, fit-for-purpose and support the achievement of the University's mission and objectives. For example, we avoid creating or collecting unnecessary information, we avoid unnecessary duplication, and we seek to avoid any information gaps that mean we do not have the details needed to achieve the University's objectives, e.g., accounting for our decisions to data subjects. Where appropriate, information is standardised, comparable and linkable to allow it to be reused so that we can maximise its value. For example, information in line of business applications is recorded consistently so data cleansing is not needed (or is minimised) before statistical analyses are carried out.
- have **Confidentiality**
  Information assets are protected from unauthorised access, disclosure, alteration, and destruction. They are as closed as necessary and as open as possible. For example, by applying role-based access permissions that are assigned and rescinded promptly in accordance with business need.
- have a defined **Lifecycle**
  Information assets have a defined lifecycle that allows the University to retain them as long as required – but no longer – and to explain why and how long

POLICY

we retain specific information assets. This includes identifying information assets with archival value as early as possible so that they can be preserved permanently. Information lifecycles are defined in the University's Retention Schedules, which support this Policy.

- are **Available**
  Authorised individuals know what information assets exist and can locate and retrieve them timeously throughout their lifecycle. For example, it is possible to identify and retrieve all the information about a specific individual to facilitate their data subject rights. The information assets are clear, concise, intelligible, and legible. They are usable by any University personnel authorised to do so, including those with protected characteristics. For example, colour is not used as the only way of conveying meaning as doing so makes the information unavailable to people with colour blindness.
- have **Integrity**
  Information assets are reliable, authentic, accurate, complete, and protected from unauthorised amendment or deletion, so that they can be trusted. For example, adequate audit trail and version history metadata is created and maintained, and evidential weight is maximised, so the University meets its audit and regulatory obligations. It is clear where the Single Point of Truth is held, who is responsible for its maintenance, and any copies are clearly identified as such. For example, the University's corporate line of business applications will normally contain the Single Point of Truth and any data extracts from them for local analysis are copies. Where appropriate, information quality standards are defined and monitored so that it can be relied on for evidence-based decision-making. For example, standards of accuracy need to be maintained for vital information in line of business applications and any errors reported.
- are **Resilient**
  Information assets are resistant to the impact of incidents that would otherwise have a serious adverse impact on their confidentiality, integrity or availability, and support business continuity.

3.3 Our use and management of our information assets is:

- **Proportionate**
  The University's use and management of information is proportionate to the purpose, benefits, and costs, and takes account of the University's risk appetite. For example, greater effort is expended managing vital information than transitory information.
- **Legal**
  The University's use of information complies with the laws in all the jurisdictions in which it operates.
- **Accountable**
  The University creates, keeps, and manages information to support its business activities and to be accountable for its actions and decisions, including compliance with legal obligations and regulatory requirements. Information Asset Owners are accountable for the governance and management of information assets produced and maintained by the functions and activities for which they are accountable.
- **Cost-effective**
  The University's use of information, and its information systems balance economy, efficiency, and effectiveness to achieve the University's mission and objectives with the optimal use of resources and are value for money over the long-term. For example, information assets are held in the medium most appropriate for the task they perform, in the most cost-effective location,

POLICY

and wherever possible and practicable routine information management activities are automated to support staff and make processes more effective and efficient. Information sources are integrated rationally so manual keying between systems is minimised. For example, student contact details are always collected against the same information schema and transferred between systems without manual intervention.

- **Ethical**
  The University's use of information is socially responsible and reflects the University's ethos, values, and heritage. For example, our use of information supports the University's contributions to the United Nations' Sustainable Development Goals.
- **Transparent**
  The University is transparent about its activities, the purposes for which it holds information and how that information is managed. All University information is discoverable and potentially disclosable, for example in response to freedom of information requests and data subject rights requests.

4. SCOPE

What information is included in the Policy

4.1 This Policy applies to **all information assets created, received, and maintained in the course of university business** by anyone working on behalf of the University, in all formats, of any age, wherever they are created, used, stored, or held. Information assets include data (and personal data), information, and records. Information assets produced in the course of university business belong to the University, rather than the individuals that created them.

For example, this Policy applies to:

- University information assets held in Microsoft 365, including SharePoint Online, OneDrive, Teams, Outlook, Yammer, Stream, Sway, OneNote, and Power Apps
- University information assets held in line of business applications hosted by the University and those hosted by third party organisations
- University information assets held on personal devices (e.g., smart phones, tablets, computers), personal IT accounts (e.g., WhatsApp, Slack, Signal, Telegram) or at home
- The conversion of a university-owned information asset from one format to another, for example scanning or 'digitising' paper records
- Non-current, legacy information

Who is affected by the Policy

4.2 The Policy applies to **everyone working on behalf of the University** (including: Employees, casual workers, contractors, agents, and those with an honorary or voluntary role) whenever they are carrying out work for the University.

Where the Policy applies

4.3 This Policy applies to **all locations** from which University information assets are created, received, used, stored, or held, including home and mobile use.

POLICY

4.4 As the University operates internationally, through its campuses in the United Kingdom, Dubai and in Malaysia and through arrangements with partners in other jurisdictions, the remit of this Policy includes our overseas campuses and international activities and shall pay due regard to applicable legislation in each relevant country.

5. LINES OF RESPONSIBILITY

5.1 **Everyone working on behalf of the University has information asset management responsibilities**. Managing the information individuals receive, create, and use when carrying out University activities is a core element of those activities. This Policy brings together and specifies those existing responsibilities:

- To **document** their work effectively by creating and maintaining records that have integrity and which support the University to be accountable for its actions and decisions
- To follow any relevant business rules, procedures or guidance provided by the Information Governance Division and their local Information Asset Manager:
    - To **create** information assets in the standardised manner agreed (e.g., using the agreed template for a particular document type, or inputting information into a system in a particular format)
    - To timeously **capture** University information assets (including emails and instant messages) in the appropriate information system with the relevant metadata (e.g., version history and naming conventions)
    - To understand the impact of their record-keeping practices on downstream systems

  so that information assets meet business requirements (including information quality requirements), are available to authorised individuals and backed-up to aid resilience.

- To follow **information security** policies and procedures to protect the confidentiality of information assets
- To apply **good housekeeping** principles by routinely and regularly disposing of transitory information as soon as it reaches the end of its lifecycle and is no longer required
- To work with their managers, local Information Asset Manager, and colleagues to apply the University's **records retention schedules** and follow disposal guidance provided by the Information Governance Division so that the University retains information assets as long as required, and documents their secure disposal or transfer to the University Museum and Archive at the end of their lifecycle
- To report any information quality issues to the relevant local Information Asset Manager
- To familiarise themselves with the University's information governance policies and procedures, and the supporting guidance provided by the Information Governance Division through the Information Governance pages on the University website and intranet
- To undertake mandatory induction **training**, and relevant refresher training provided by the University to support compliance with this Policy
- To arrange **orderly handover** of information assets and responsibilities to their manager before leaving the University

POLICY

5.2 **The Secretary of the University** has senior management accountability for information governance, reporting to the University Executive and the Audit and Risk Committee on relevant risks and issues.

5.3 **The Global Director of Governance and Legal Services** has senior management responsibility for information governance.

5.4 **The Head of Information Governance** (IG) is responsible for recommending information governance and records management strategy and policies to the Global Director of Governance and Legal Services, with the advice of the Records Manager, and leading the Information and Records Management Programme (see section 7 below), promoting good practice, monitoring compliance, and recommending revisions to these policies in line with business need, legal requirements, and professional standards.

5.5 **The Records Manager** is the functional lead on all matters relating to records management. They have operational responsibility for developing the Information and Records Management Programme (see section 7 below) and supporting its implementation. This includes providing advice and guidance to support and promote good practice, and recommending revisions in line with business need, legal requirements, and professional standards.

5.6 **The Global Director of Information Services** is accountable for working collaboratively with the Information Governance Division and functional leads to plan and develop information systems to achieve this Policy's objectives and meet the information governance principles (see section 3 above). This includes:

- Maintaining University IT systems to ensure information assets held within them remain effective, retain their confidentiality, availability, integrity, and resilience, and have a defined lifecycle, throughout any system change, including format conversion, migration between hardware and operating systems or specific software applications. For example, by providing the framework for assigning and rescinding role-based access to information assets and systems
- Managing the information lifecycle of information assets held in centrally managed information systems, especially line of business applications. For example, agreeing an exit strategy so that retention and preservation requirements are identified and met
- Senior management responsibility for the University Museum and Archive Service

5.7 **Information Asset Owners** are accountable for the governance and management of information assets created, received, used, and maintained by the University functions and activities for which they are accountable, by:

- Championing the information governance principles (set out in section 3 above)
- Fostering a culture that values information and its good governance
- Managing information risks using the University's risk management framework
- Ensuring those working on behalf of the University undertake appropriate mandatory and role-based information governance training and have appropriate information access for their roles

POLICY

- Ensuring the Information Asset Manager responsibilities are appropriately allocated and carried out
- Supporting Information Asset Managers to carry-out their role, for example through the provision of appropriate resources and recognition
- Endorsing business rules for managing information assets falling within their area of accountability

Appendix 2 sets out an indicative Information Asset Owner role description.

5.8 **Information Asset Managers** are responsible for supporting their school or professional service to implement the Information Governance Principles (see section 3 above) to comply with this Policy and related procedures and guidance, in relation to the information assets and information systems for which they are responsible. This Policy formally recognises and describes this role that has previously been undertaken under different names and establishes a framework of support for the colleagues undertaking it. Appendix 3 sets out an indicative Local Information Asset Manager (LIAM) role description.

5.9 **Project sponsors and board members** are accountable for implementing this Policy and supporting procedures for the projects they oversee. All University projects involve the creation and use of university information assets to a greater or lesser extent. It is especially important that projects involving information systems and processes include sufficient resource to address information governance requirements and that this is part of the project bid. Proper consideration of information governance requirements must begin as early as possible so that timely adjustments to project implementation can be made to comply with the University's legal, regulatory and accountability obligations. Project sponsors and board members must satisfy themselves that information governance risks and requirements have been fully considered (e.g., through completion of the Information Governance and Data Protection Impact Assessment Toolkit) and relevant actions implemented.

5.10 **Project managers** are responsible for implementing this Policy and the supporting procedures when planning and implementing projects. This includes keeping project sponsors and board members fully informed of information governance risks and issues (e.g., risks identified through completion of the Information Governance and Data Protection Impact Assessment Toolkit).

5.11 **All managers** are responsible for implementing this Policy and the supporting procedures within their areas, and for adherence by their staff. This includes:

- Ensuring adequate records are kept of the activities for which they are responsible
- Fostering a record-keeping culture so that the University is accountable for its actions and decisions and has the information it needs to provide quality services, support good governance and quality decision making
- Assigning generic and specific responsibilities for information governance and records management
- Working collaboratively to contribute to the development of business rules for the activities they manage, and supporting their staff to follow the agreed business rules
- Working collaboratively with the Information Governance Division to agree and apply records retention schedules, transfer, and disposal arrangements for their areas of responsibility

- Managing access rights for information assets and systems to ensure those working on behalf of the University have access only to such confidential information assets as necessary for them to fulfil their duties
- Giving all staff in their area sufficient time within their working hours to undertake relevant training provided by the University and are aware of their accountability for information governance
- Ensuring staff responsible for any locally managed IT services work with colleagues in the Information Services Directorate and Information Governance Division to achieve this Policy's objectives

5.12 This Policy recognises the University is on a continuous journey of improvement. Individuals must feel able to report any concerns they may have and receive support to fulfil their responsibilities. Support mechanisms will be developed through the Information and Records Management Programme (see section 7 below).

5.13 Compliance with this Policy supports the University to comply with legal and regulatory requirements that are embedded in other university policies. Failure to comply with aspects of this Policy could lead to a failure to comply with those requirements. For example, oversharing confidential information would be a data breach under the Information Security Policy Framework, failure to retain and delete personal data in accordance with agreed retention and disposal policies would be a data protection breach, and in some circumstances deletion of information subject to a freedom of information request is a personal criminal offence. Consequently, continued, or deliberate failure to comply with this Policy will be treated as misconduct and subject to investigation under the appropriate campus University Disciplinary Policy.

6. MONITORING AND EVALUATION

6.1 The **Head of Information Governance** monitors the implementation of this Policy and the underpinning Information and Records Management Programme (see section 7 below), reports on progress to the **Global Director of Governance and Legal Services** and considers measures to enhance effective information management and responds to developments in the regulatory and risk environment.

6.2 The **Global Director of Governance and Legal Services** owns the strategic information governance risk. The **Global Director of Information Services** owns the strategic cyber security risk. The **Head of Information Governance** liaises with the **Head of Assurance Services** to advise the Global Directors to ensure information governance risks are captured and adequately monitored at local and strategic levels.

6.3 The **Records Manager** provides University-wide advice, guidance and training and has overall day-to-day responsibility for developing the Information and Records Management Programme (see section 7 below) and supporting its implementation by working collaboratively in partnership with Information Services, schools, professional services, and local Information Asset Managers.

6.4 Each **Information Asset Owner** will nominate at least one **Local Information Asset Manager** for their area of accountability. The **Records Manager** will maintain a register of Information Asset Managers and inform Information Asset Owners of any gaps in coverage.

6.5 The **Records Manager** will provide guidance and training to **Local Information Asset Managers** to equip them with the knowledge and skills to perform the responsibilities outlined in Appendix 3.

6.6 Each **Local Information Asset Manager** will make an annual return to the **Records Manager** providing an assessment of the information management maturity of their area of responsibility. The Records Manager will review the assessments, collate a report for the Global Information Governance and Data Protection Committee, and provide feedback to Local Information Asset Managers and Information Asset Owners.

6.7 The following groups will contribute to monitoring and evaluating the effectiveness of this Policy and provide feedback on how it can be strengthened, from their specific governance, specialist, and stakeholder perspectives.

6.8 The **Global Information Governance and Data Protection Committee** (GIGDPC) reviews and recommends information governance, data protection and security related policies and procedures, monitoring the effectiveness of controls and recommending measures to comply with legal obligations, optimise the effective use of information assets including data quality standards to support the University Strategy, and maintain information assets consistent with the Information Governance Principles (set out in section 3 above).

6.9 The **Global Operations Executive** (GOE) advises on the effective management of the University's assets and resources in the context of delivery of the University's Strategic Plan and develops and maintains common approaches and standards across the University, for example by sharing and proactively taking up best practice.

6.10 The **Infrastructure Committee** has oversight of the stewardship and development of the University Museum and Archive Collections. In this capacity the Committee ensures that appropriate provision exists for the preservation, accommodation, and access to the University's heritage collections.

6.11 The **Infrastructure Services Management Board** provides a management forum to deliver Infrastructure Services. The Board has oversight of the University's global IT infrastructure, development, support, and business continuity plan.

7. IMPLEMENTATION

7.1 This Policy is implemented through a continuous and incremental **Information and Records Management Programme**. The Programme is intended to help users to do the right thing with information by default. The core elements of the programme are described below and are based on the key elements of good practice set out in the Freedom of Information (Scotland) Act 2002, section 61 Code of Practice on Records Management, and are informed by the Model Records Management Plan issued under section 1 of the Public Records (Scotland) Act 2011. The five-year programme outlined below will be revised during the next review of this Policy.

7.2 This Policy recognises information management maturity levels differ throughout the University and that all areas of the University are on a continuous, incremental

journey of improvement which will be monitored and recognised using an annual information management maturity assessment.

7.3 The Information and Records Management Programme is led by the Information Governance Division working collaboratively in partnership with Information Services, schools, professional services, Information Asset Managers, and Information Asset Owners.

7.4 Some elements of this programme also form part of the Information Security Management Programme developed under the Information Security Policy Framework, and the Global Privacy Programme developed under the Data Protection Policy.

7.5 The Strategic Planning, Performance and Projects Directorate will lead the development of a framework to support the management of structured information in line of business applications, which will operate alongside the Programme outlined below. The framework will include the development of a business glossary to provide a common language to underpin discussions, and a process for logging and resolving issues (e.g. information quality issues).

Information and Records Management Programme

7.6 **Identify Information Asset Owners** and brief them on their responsibilities as described in Appendix 2.

7.7 **Establish a support network for Local Information Asset Managers** and provide guidance and training to members of the network to support them in their role. Local Information Asset Managers will provide a crucial link to implement the Information Governance Principles (see section 3 above) through the Information and Records Management Programme and enable the effectiveness of the Programme to be monitored and evaluated.

7.8 **Promote good information asset management practices to all staff and foster an effective record-keeping culture** through:

- Mandatory induction training
- Refresher training
- Leaver management procedures and awareness raising
- Provision of awareness raising resources to Local Information Asset Managers for cascade to their area of responsibility

7.9 Work collaboratively to **develop, document, and promote business rules for the University's principal activities**. Business rules enable the objectives of this Policy to be embedded in business processes pragmatically and consistently. Business rules may be documented as formal procedures under this Policy, such as the Student Records Procedures, or may be documented locally as standard operating procedures. The documentation method will vary according to the number of teams that need to follow the business rules and the level of information governance risk.

7.10 Work collaboratively to **develop, maintain, and promote good practice in the development and use of information systems,** such as:

POLICY

- Line of business applications, e.g., Banner, Oracle ERP, Worktribe, Canvas virtual learning environment (VLE), Pure, customer relationship management systems (CRM)
- M365 Workspaces for semi-structured digital records, in accordance with the Office 365 Policy
- A trusted digital repository for semi-current digital records that require active digital preservation to ensure their resilience, in accordance with the Digital Preservation Policy
- The Records Storage & Retrieval Service for semi-current physical records

7.11 Work collaboratively to **embed information governance principles into all new and upgraded information systems and applications** by promoting the use of the Information Governance and Data Protection Impact Assessment Toolkit. The Toolkit is an essential part of the University's Global Privacy Programme to embed data protection by design and default, one of the University's statutory duties.

7.12 Work collaboratively to begin to **develop an information asset register**, building on the existing Records of Processing Activities and the HE business classification scheme developed by JISC. An information asset register will provide an overview of the University's information assets, which will enable the Information Governance Division to provide prioritised and targeted support to manage information governance risks. For example:

- Identifying the Single Point of Truth, and any shadow systems
- Providing the basis to collate information about the University's vital information for business continuity planning

7.13 Work collaboratively to **maintain, develop, and promote appropriate disposal arrangements**. This includes:

- Reviewing and updating the University's retention schedules to ensure they remain up to date and effective
- Developing disposal guidance to help schools and directorates implement the University's retention schedules consistently, securely and maintain records of destruction
- Developing archival transfer arrangements for digital and physical records, to ensure an adequate historical record is maintained in accordance with the Collections Development Policy and the Digital Preservation Policy
- Promoting the use of the University's retention schedules, disposal guidance and archival transfer arrangements to raise colleagues' awareness of what they need to do, particularly where they are creating records which have been identified for transfer to the University Museum and Archive

7.14 Work collaboratively to **maintain, develop, and promote information security good practice**. This includes:

- Maintaining the University's Information Security Classification Scheme and promoting its use
- Providing guidance on managing access to university information assets, including how to put in place adequate controls to prevent unauthorised access, destruction, alteration, or removal of information assets
- Supporting the implementation of the Information Security Policy Framework

POLICY

7.15 Work collaboratively to **maintain, develop, and promote good information governance practice when sharing information externally**. This includes:

- Developing data sharing guidance so that all information sharing is lawful, secure, and documented, e.g., using one of the University's template data sharing agreements
- Promoting the use of data sharing agreements (e.g., the University's template data sharing agreements) for sharing University information with third parties who are not working on behalf of the University
- Developing guidance and processes to support supplier due diligence before signing a contract, and continuous contract management after signing a contract, with any supplier that processes University information assets on behalf of the University to gain assurance that the supplier maintains appropriate organisational and technical measures to protect the information assets and comply with its duties to the University
- Putting in place appropriate data processor agreements (e.g., the University's template data processor agreements) for any relationships with suppliers or contractors that include processing personal data on behalf of the University
- Promoting the University's publication scheme and appropriate proactive publication
- Responding to requests for information (e.g., freedom of information requests) in a fair, friendly, and timely manner, while also protecting confidential information by appropriate use of exemptions

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCES

Strategies

8.1 This Policy supports Strategy 2025 and the following enabling strategies:

- Data Strategy (forthcoming)
- Digital Strategy (forthcoming)

Policies

8.2 This Policy should be read in conjunction with all other University information governance policies, which are reviewed and updated as necessary to meet the University's business needs and legal obligations. Relevant policies are published on the University website at: https://www.hw.ac.uk/uk/about/policies.htm. These include:

- Data Protection Policy
- Digital Preservation Policy
- Information Security Policy Framework, and its constituent policies and procedures
- IT and Communications Facilities Acceptable Use Policy
- Museum and Archive Collections Development Policy
- Office 365 Policy: Online collaboration, communication, and document storage
- Research Data Management Policy

8.3 This Policy should also be read in conjunction with University's Risk Management Framework. Information assets are corporate assets, and their loss or compromise disrupts University business. The Risk Appetite statement sets out the University's

zero risk appetite for breaches of legislation, regulations or professional standards, and the University's cautious approach to risks around the management and storage of information.

Procedures

8.4 This Policy should be read in conjunction with university information governance procedures, which are reviewed and updated as necessary to meet the University's business needs and legal obligations. Relevant procedures are published on the University website at: https://www.hw.ac.uk/uk/about/policies.htm. These include:

- Information Governance and Security – Leaver management checklist for managers
- Procedures for selecting digital formats
- Procedures for responding to requests for personal data
- Student records procedures
- Retention schedules

Legal requirements

8.5 Effective information governance is essential for compliance with law in all jurisdictions in which the University operates. This Policy supports compliance with any legal or regulatory requirement which requires the University to:

- Provide access to information assets it holds, or which are held on its behalf by a third party. For example, freedom of information and data protection law
- Maintain the confidentiality of information. For example, data protection law and common law duty of confidentiality
- Retain or dispose of information assets within a specific time frame. For example, immigration rules, finance law, employment law, data protection law, research funder requirements, charity law, health and safety regulations
- Justify the retention or not of specific information assets. For example, freedom of information and data protection law

8.6 Legislation that places specific information governance and record-keeping obligations on the University includes, but is not limited to:

- Freedom of information laws:
  - Freedom of Information (Scotland) Act 2002 (FOISA)
  - FOISA section 61 Code of Practice on Records Management
  - FOISA section 60 Code of Practice on Discharging the Functions of Public Authorities
  - Environmental Information (Scotland) Regulations 2004
- Data protection laws:
  - UK Data Protection Act 2018
  - UK General Data Protection Regulation
  - Malaysia Personal Data Protection Act 2010
  - UAE Federal Law No.45/2021 On the Protection of Personal Data (PDPL)
- Privacy and electronic communications laws:
  - UK Privacy and Electronic Communications Regulations 2018

POLICY

- UAE Penal Code, articles 378-379
- UAE Constitution, article 31
- UAE Federal Law No.3/2003 On Organising the Telecommunications Sector
- UAE Federal Law No.5/2012 On Combating Cyber Crimes

UK Home Office Immigration Rules, and the accompanying Sponsorship guidance for employers and educators

External standards

8.7 This Policy supports compliance with the following British and international standards:

- BS 10025:2021 Management of records – Code of practice
- BS ISO 15489 Information and documentation. Records Management
- BS ISO 23081:2017 Information and documentation. Records management processes – Metadata for records
- BS ISO 30300 Information and documentation. Management systems for records
- BS EN 15713:2009 Secure destruction of confidential material. Code of practice
- BS 10008 Evidential weight and legal admissibility of electronically stored information
- BS ISO /IEC 27001 Information Security Management
- ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- BS 10010:2017 Information classification, marking and handling
- BS EN ISO 22301:2019 Security and resilience. Business continuity management systems. Requirements
- BS 4971:2017 Conservation and care of archive and library collections
- BS EN 16893:2018 Conservation of Cultural Heritage – Specifications for location, construction and modification of buildings or rooms intended for the storage or use of heritage collections
- Payment Card Industry Data Security Standard (PCI DSS)

British standards are available to members of the University Library through the Library's subscription to British Standards Online (BSOL).

8.8 This Policy supports compliance with sectoral standards and best practice. For example, the Higher Education Achievement Report (HEAR), Enhancement Led Institutional Review (ELIR), and research funder policies.

8.9 This Policy is supported by records retention schedules, business classification scheme, and records management maturity self-assessment, which are based on the following higher education standards of good practice:

- JISC: Records retention management: https://www.jisc.ac.uk/guides/records-retention-management
- JISC: Records management maturity model: https://www.jisc.ac.uk/guides/records-management/maturity-model

POLICY

Impact assessments

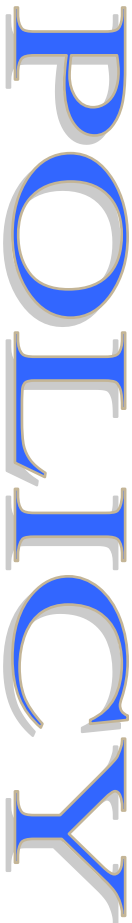
8.10 The equality impact assessment for this Policy is provided in Appendix 5.

8.11 The data protection impact assessment screening questionnaire for this Policy is provided in Appendix 5.

9. DEFINITIONS

9.1 This section provides definitions for terms used in this Policy.

Archival value	Long-term research value for cultural purposes. Probably less than five percent of the University's information assets have archival value and need to be preserved permanently in the University Museum and Archive. Information assets with archival value are those which reflect and provide the essential evidence of the University's most significant functions and activities, and also serve legitimate research needs of the University and wider academic and public user community. Information with archival value collectively shows how the University was organised and operated, its effect on the wider community and what it did and why.
Archives	Records which have been created or received by the University in the course of its activities and functions and selected for permanent preservation by the University Museum and Archive in consultation with the records creators.
Business rules	The rules that set out what information needs to be kept to meet business, regulatory, legal and accountability purposes. The Information Asset Owner should endorse the rules. The rules should set out: • What information should be kept • By whom this should be done • At what point in the process this should be done • What the information should contain • Where and how it should be stored • The information security and vital information classifications and how the information will be protected In developing the rules consideration must be given to: • Legislative and regulatory requirements • The need to document actions and decisions to support current business needs and accountability requirements • Downstream information uses



- The need to protect the rights of the University, staff, students, and other stakeholders
- Compliance with the information governance principles (see section 3 above)

Confidential information

Any information to which a disclosure exemption would apply under freedom of information law. This includes but is not limited to:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent
- Information received in confidence from third parties (e.g., industrial partners) where disclosure would be an actionable breach of confidence
- Information which would significantly harm the University's ability to conduct its legitimate activities
- Information which would significantly damage the University's commercial interests or the commercial interests of a third party if it were disclosed without authorisation

Further examples can be found in the University Information Security Classification Scheme

Data

Information, especially facts or numbers, examined and considered and used in calculating, reasoning, discussion, planning or decision-making. Often held in electronic form that can be stored and used by a computer. Data can be considered the building blocks of 'information'.

Data protection by design and default

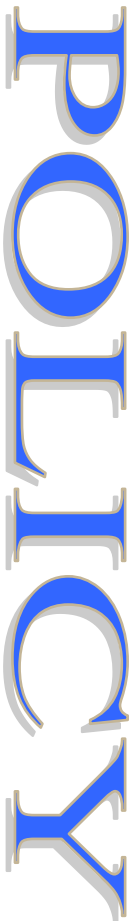
Under data protection law the University has a statutory duty to apply appropriate technical and organisational measures to embed (by design and default) the data protection principles into all our activities involving personal data and protect the rights of data subjects.

"By design" means "baking-in" data protection principles to all our systems and processes.

"By default" means that as a matter of course only personal data which are necessary for each specific purpose are processed. This relates to the amount of personal data collected, the extent of the processing and their retention. For example, by default social media settings are set to 'private'.

POLICY

Information	Details (data, facts, opinions etc.) about something. Information is sometimes defined as data endowed with meaning and purpose. Information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.
Information asset	An information asset may comprise a combination of data, electronic or paper documents, still or moving images, objects, hardware, and software that together support a university activity. The term is broad. The National Archives defines an information asset as: "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles."
Information asset owner (IAO)	The senior manager accountable for the business function or activity to which the information assets relate. The role description is provided in Appendix 2 below.
Information asset register (IAR)	Metadata about the University's information assets that is kept up to date and collated in one place so that it can be analysed and interrogated. At a minimum: asset name, asset location, asset owner. Normally linked to records of processing activities, retention schedules, business classification scheme and information security classification. The National Archives defines an information asset register (IAR) as: "a simple way to help you understand and manage your organisation's information assets and the risks to them. It is important to know and fully understand what information you hold in order to protect it and be able to exploit its potential."
Information governance	Information governance is the framework of accountability, processes, and controls to support the effective management of information throughout its lifecycle to meet organisation's business needs and legal and stakeholder obligations. It incorporates the creation, management and destruction of information, information security, privacy, access rights and legal discovery.



Information security classification scheme	The University's "Red Amber Green Data Safety Code" which identifies confidential information based on the level of harm that would result if the information were lost, stolen, or accidentally disclosed to others. The scheme provides examples of the main kinds of information used by the University in each category and gives practical advice on what to do to store the information, communicate the information and securely destroy the information when no longer needed. The Scheme is available at Information Security Classification Scheme
Information system	Any system which captures, manages, and provides access to university information assets, including line of business applications. An information system may consist of technical elements such as software and non-technical elements including procedures, guidance, people and assigned responsibilities. Systems may be digital and complex where many of the information management activities can be automated, or a simple paper-based system where information management activities are performed manually according to agreed procedures. Examples of information systems used by the University include: Banner; Oracle ERP; Worktribe; Canvas virtual learning environment (VLE); customer relationship management systems (CRM); M365 Workspaces; Records Storage & Retrieval Service.
Local information asset manager (LIAM)	The member(s) of staff appointed by directors of professional services and heads of operations in schools to support their professional service or school to implement the information governance principles (see section 3 above) to comply with this Policy and related procedures and guidance. The role description is provided in Appendix 3 below.
Metadata	Information about information. Information assets comprise content and metadata. Metadata is essential for demonstrating the integrity of information assets, and helps to make information assets more findable (available) and resilient. Metadata describes the context, content, and structure of information assets, as well as their management through time. Metadata describes the business context in which an information asset was created or received and used, the relationships with other information

POLICY

assets, and provides information necessary to retrieve and present the information asset. Metadata items include:

- File name / file title
- File type (e.g., .pdf, .docx, .xlsx, .pptx)
- Information asset creator or author
- When the information asset was created
- Which business process created the information asset
- Which business function and activity the information asset relates to
- Information about the format of the information asset
- Information about the location of the information asset
- Version history information
- Access restriction information

Metadata may be structured or semi-structured information. It may be captured as part of the information asset or may be held separately.

Personal data

Information in any format that relates to an identified or identifiable living person. An identifiable living person is someone who can be identified directly or indirectly from an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Although the UK GDPR and the Data Protection Act 2018 apply only to living people, the scope of this policy also includes information about deceased individuals. This is because disclosure of information about the deceased may still be in breach of confidence or otherwise cause damage and distress to living relatives and loved ones.

Record

Recorded information or data (in any format) created, received, or maintained by the University (or someone working or acting on its behalf) in the transaction of university business or conduct of university affairs and kept as evidence of those activities for business, regulatory, legal or accountability purposes.

'Business purposes' are any purposes which support the University's functions and activities. 'Regulatory purposes' are any purposes which support or demonstrate the University's compliance with regulatory requirements. 'Legal purposes' are any purposes which support or demonstrate the University's compliance with any legal obligation. 'Accountability purposes' are any

POLICY

	purposes whereby the University answers for its conduct.
Records management	Records management is a key component of information governance. It is the "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records." BS ISO 15489.
Records of processing activities (RoPA)	Under data protection law the University has a statutory duty to maintain detailed records of its personal data processing activities and make them available on request. The requirement is set out in Article 30 of the UK GDPR.
Records Storage & Retrieval Service (RS&RS)	A service that allows schools and professional services in Scotland to store their semi-current physical records securely off-site, for authorised users to retrieve them whenever they are needed, and for them to be securely destroyed at the end of their retention period. The service is provided under contract by an external supplier. The contract is managed by the Information Governance Division.
Retention schedule	Sets out the agreed length of time the University needs to keep different types of records. Retention schedules are policy documents which support compliance with legislative and regulatory requirements. The University's retention schedules are available at: University Retention Schedules.
Transitory information	Has only temporary value. It is produced: • In the completion of routine actions (ephemeral records) • In the preparation of other records which supersede them (temporary records) • For convenience of reference (reference copies) Transitory information has no significant informational or evidential value after it has served its primary purpose. It can usually be disposed of within no more than 6 months.
Vital information	Information that enables the University to perform its core functions or provide evidence that the University has performed its core functions. This information is

POLICY

crucial to the conduct of the University's business, without it the University could not continue to operate.

Identifying and protecting the University's vital information is an important part of business continuity planning and disaster management.

10. FURTHER HELP AND ADVICE

10.1 For further information and advice about this Policy and any aspect of information and records management or information governance contact:

Ann Jones
Head of Information Governance and Data Protection Officer

Anne Grzybowski
Records Manager

Information Governance Division
Governance and Legal Services
Telephone: 0131 451 3219 / 4140
Email: InfoGov@hw.ac.uk

11. POLICY VERSION AND HISTORY

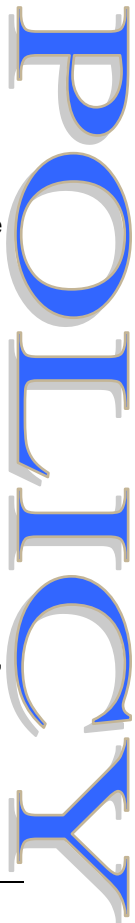
Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V4 21/02/2014	Supersedes policy approved April 2002	Secretary's Board	Revisions to take account, legal, technological, business and risk environment; minor amendments to Lines of Responsibility following consultation
V10	19 April 2022	University Executive	Substantial revisions to take account of Strategy 2025 (section 2), the development of the Information Governance Principles (section 3), changes to the University's governance structures (section 5), update the Records Management Programme (section 7) to bring it explicitly in line with the Scottish Ministers' Code of Practice on Records Management By Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002, addition of relevant UAE privacy laws and related

POLICY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
			forthcoming University strategies (section 8).

12. APPENDIX 1: POLICY SUMMARY

Our information assets are precious	They comprise a combination of recorded details (data, facts, opinions, etc.) that support a University activity or function. They provide evidence of our actions, rights, and entitlements. They also support innovation, collaboration, and are a fundamental building block of knowledge. The Information Governance and Records Management Policy applies to all information assets created, received, and maintained in the course of University activities, whatever their age, format, storage or global location.
We will apply Information Governance Principles to make the most of our information assets	Our information assets, like other assets (e.g. money, people, buildings), need to be managed to get the most from them. Applying the Information Governance (IG) Principles will help us to do so. The IG Principles are set out in section 3 of the Policy and summarised below. We create, receive, and maintain information assets that:
are **Effective**	Information assets are consistent, fit-for-purpose and support the achievement of the University's mission and objectives. Where appropriate, information is standardised, comparable and linkable to allow it to be reused so that we can maximise its value.
have **Confidentiality**	Information assets are protected from unauthorised access, disclosure, alteration, and destruction. They are as closed as necessary and as open as possible.
have a defined **Lifecycle**	Information assets have a defined lifecycle that allows the University to retain them as long as required – but no longer – and to explain why and how long we retain specific information assets. We do this through the University's Retention Schedules.
are **Available**	Authorised individuals know what information assets exist and can locate and retrieve them timeously throughout their lifecycle. The information assets are clear, concise, intelligible, and legible. They are usable by any University personnel authorised to do so, including those with disabilities.
have **Integrity**	Information assets are reliable, authentic, accurate, complete, and protected from unauthorised amendment or deletion. Where appropriate, information quality standards are defined and monitored so that it can be relied on for evidence-based decision-making.



are **Resilient**	Information assets are resistant to the impact of incidents that would otherwise have a serious adverse impact on their confidentiality, integrity or availability, and support business continuity

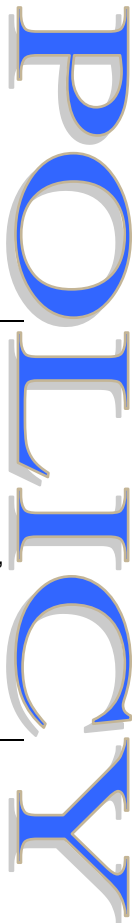
Our use and management of our information assets is:

Proportionate	The University's use of information is proportionate to the purpose, benefits, and costs, and takes account of the University's risk appetite.
Legal	The University's use of information complies with the laws in all the jurisdictions in which we operate.
Accountable	The University creates, keeps, and manages information to support our business activities and to be accountable for our actions and decisions, including compliance with legal obligations and regulatory requirements.
Cost-effective	The University's use of information, and our information systems balance economy, efficiency, and effectiveness to achieve the University's mission and objectives with the optimal use of resources and are value for money over the long-term. Information sources are integrated rationally so manual keying between systems is minimised.
Ethical	The University's use of information is socially responsible and reflects the University's ethos, values, and heritage.
Transparent	The University is transparent about its activities, the purposes for which we hold information and how that information is managed. All University information is discoverable and potentially disclosable, for example in response to freedom of information requests and data subject rights requests.

The IG Principles support our mission and objectives	Our university's mission is "to create and exchange knowledge that benefits society". Our information assets are fundamental building blocks for the development of knowledge. Section 2 of the Policy sets out the ways applying the IG Principles will deliver the University's strategic objectives, meet legal, compliance and accountability obligations, manage risks in line with our risk appetite, support business continuity and protect the University's corporate memory and historical record.

POLICY

The IG Principles make our working lives easier	We will have timely access to reliable, authentic, accurate, and trustworthy information that we need to do our jobs, wherever we work and whatever our role. We'll be able to get straight to work, without first needing to overcome information quality or availability hurdles. We will know what information assets exist and where they are so our innovations can benefit from the University's previous experience and we can find synergies with colleagues working elsewhere on similar topics. We'll know what information to keep, where to keep it and with whom it can be shared, so we can focus on our work that really adds value.
Everyone working on behalf of the University has a role to play, including you	Managing the information we receive, create, and use when carrying out work for the University is a core element of our work, and always has been. Our responsibilities are set out in paragraph 5.1 of the Policy. But you're not on your own, you will be supported to help you fulfil your responsibilities.
Some roles have specific responsibilities	People managers, project managers, project sponsors, and members of project boards all have important roles to play in implementing the Policy within their areas. Their responsibilities are set out in paragraphs 5.9-5.11 of the Policy.
Some roles have formal recognition for the first time	Senior managers accountable for a business function (e.g., HR, Finance, Research) have always been accountable for the information produced and used by that function. These information governance accountabilities are formally recognised for the first time with the title 'Information Asset Owner', and a role description is provided in Appendix 2 of the Policy. Some colleagues have always had a role in supporting their teams' information management, for example by arranging for files to be destroyed or transferred to offsite storage at the end of the year. This role is just as important in our digital environments, and it is now formally recognised with the title 'Local Information Asset Manager'. The role description is provided in Appendix 3 of the Policy.
Implementation will be gradual, and support will be provided	The University is on a continuous journey of incremental improvement. We will reach our objective to apply the IG Principles by implementing the Information and Records Management Programme outlined in section 7 of the Policy. The Information Governance Division will lead the Programme, which includes revitalised training and awareness raising resources, new tools, and support for all colleagues and especially those with specific roles and responsibilities under the Policy. Follow the Information Governance Intranet Hub to keep up to date with the latest information governance news.



13. APPENDIX 2: INDICATIVE INFORMATION ASSET OWNER ROLE DESCRIPTION[1]

Role purpose

13.1 To provide leadership and accountability for governing and managing the information assets created, received, used, and maintained by the University functions and activities for which they are accountable.

Background

13.2 Effective and efficient information asset management (including data, information, and records) underpins all the University's functions and activities and supports the delivery of the University's strategic priorities. The Information Governance and Records Management Policy also supports the University to meet the Scottish Ministers' Code of Practice on Records Management By Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002.

Identification

13.3 The Information Asset Owner (IAO) is the senior manager accountable for the business function or activity to which the information assets relate. IAOs will generally be the head of the relevant business function, but there may be a limited number of exceptions where it is appropriate for a lower-level manager to be an IAO. For example:

Role	IAO for information assets that include…
Global Director of Human Resources	Those relating to potential, current, and former employees, casual workers, and contractors
Global Chief Financial Officer	Those relating to financial, estates, and facilities management
Global Director of Research Engagement	Those relating to the Research Excellence Framework (REF), research and business development
Global Academic Registrar	Those relating to students
Head of Development and Alumni	Those relating to alumni and supporters
Global Director of Strategic Planning, Performance and Projects	Those relating to planning, performance monitoring, external reporting, and strategy development

POLICY

[1] This role description is indicative only and will evolve to take account of Data Strategy developments

Global Director of Governance and Legal Services	Those relating to corporate governance and compliance

Support

13.4 The Information Governance Division will brief IAOs and provide advice and guidance to support them to carry-out their role.

13.5 Where an IAO's remit includes structured information in line of business applications, support will also be provided through the framework being developed by the Strategic Planning, Performance and Projects Directorate.

Workload

13.6 Information Asset Owners need to carry out the responsibilities described below. The time commitment will vary depending on the size and complexity of their functional area.

Responsibilities

13.7 Champion the information governance principles that are set out in section 3 of the Information Governance and Records Management Policy.

13.8 Foster a culture that values information and its good governance.

13.9 Manage information risks using the University's risk management framework.

13.10 Ensure those working on behalf of the University on the functions and activities for which they are accountable undertake appropriate information governance training and have appropriate information access.

13.11 Ensure the Local Information Asset Manager responsibilities are appropriately allocated and carried out.

13.12 Support Local Information Asset Managers to carry-out their role, for example through the provision of appropriate resources and recognition.

13.13 Direction and oversight of the activities required by the framework being developed by the Strategic Planning, Performance and Projects Directorate.

13.14 Endorse business rules for managing information assets falling within their area of accountability. This includes endorsing vital information classifications and (where IAO's remit includes structured information in line of business applications) data glossary definitions.

13.15 For structured information in line of business applications, the IAO is also responsible for:

POLICY

- Approving new uses of information assets based on an assessment of the data protection and other risks. For example, new 'downstream' uses, new analyses, and new reuses
- Approving requests to create new information or amend existing information, to avoid creating duplicate or inconsistent information
- Approving new requests for one-off and regular sharing of information with restricted permissions
- Participating and engaging with relevant internal groups to co-ordinate activities and sharing information

POLICY

14. APPENDIX 3: INDICATIVE LOCAL INFORMATION ASSET MANAGER ROLE DESCRIPTION[2]

Role purpose

14.1 To support their Information Asset Owner and their school or professional service to implement the Information Governance Principles (see section 3 above) to comply with the Information Governance and Records Management Policy and related procedures and guidance.

Background

14.2 Effective and efficient information asset management (including data, information, and records) underpins all the University's functions and activities and supports the delivery of the University's strategic priorities. The Information Governance and Records Management Policy also supports the University to meet the Scottish Ministers' Code of Practice on Records Management By Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002.

Appointment

14.3 The Information Governance Division will ask Information Asset Owners (IAOs) to use the Information Governance Responsibilities Questionnaire to appoint at least one Local Information Asset Manager (LIAM) for their area of accountability.

14.4 The number of individuals appointed to the role will vary depending on the size and complexity of the school or professional service. The role's responsibilities may be shared between more than one individual, so long as the division of responsibilities is clear. Different individuals may hold the role for different activities or for different information systems. For example, the person responsible for the service or school's Microsoft 365 Workspace (who holds the 'Activity Manager' role under the Office 365 Policy) may be the LIAM for the Workspace only, a different person may be the LIAM responsible for physical records, and another person may be the LIAM responsible for structured information held in a line of business application.

14.5 Local Information Asset Managers must have, or be able to develop, a good knowledge of the work of their area, the information their area holds and the uses to which the information is put.

14.6 If a Local Information Asset Manager is not specifically appointed, the Information Governance Division will record the relevant service head or head of operations in schools as the Local Information Asset Manager.

Workload

14.7 Local Information Asset Managers need to carry out the responsibilities described below. The time commitment will vary considerably depending on the size and complexity of their school or professional service whether they are sharing the responsibilities with others. Approximate time commitments are provided below.

POLICY

[2] This role description is indicative only and will evolve to take account of Information Strategy developments

Where a range is given the lower end of the range is the expected commitment for smaller or simpler information governance arrangements.

Responsibilities

14.8 Attend training and awareness raising events provided by the Information Governance Division to support them in their role, and familiarise themselves with the University's information governance policies, procedures, and guidance.

Time commitment: Up to a day each year.

14.9 Annually assess the information management maturity of their school or professional service using the toolkit that will be provided and submit a copy of the completed self-assessment to the Information Governance Division.

Time commitment: Approximately 1-4 hours each year.

14.10 Work with the Records Manager to establish business rules for keeping records that relate to the activities within their area of responsibility.

Time commitment: Initial development may take 1-5 days, less where procedures already exist.

14.11 Work with the Records Manager to review and update retention periods for information assets that relate to the activities within their area of responsibility.

Time commitment: Approximately 1-7 hours each year.

14.12 Work with colleagues in their school or professional service to implement the University's retention schedules and maintain appropriate records of disposals.

Time commitment: Varies considerably depending on the information systems used by the school or professional service. For example, applying appropriate retention labels that automatically delete content at the end of the retention period to SharePoint document libraries may only take a few moments each month, and requesting the secure disposal of physical records stored in the Records Storage and Retrieval Service may take an hour each year. Other information systems may require considerable manual effort.

14.13 Work with colleagues in their school or professional service to manage and maintain information systems in compliance with university policies. This includes, for example, assigning and rescinding role-based access permissions.

Time commitment: Varies considerably depending on the information systems used by the school or professional service. For example, paper systems are likely to involve transferring semi-current records to the Records Storage & Retrieval Service once a year, which involves ordering boxes, packing boxes, adding details of the content of each box into the database and arranging for the boxes to be picked up.

14.14 Work with the Information Governance Division to review, update and build on the records of processing activities, so that the University has an overview of the University's information assets.

POLICY

Time commitment: Approximately 1-4 hours each year.

14.15 Work with the Information Governance Division to embed the Information Governance Principles (see section 3 above) into all new and upgraded information systems using the Information Governance and Data Protection Impact Assessment Toolkit.

Time commitment: Varies considerably depending on the size and scope of the new process or system being introduced but only applies when new processes or systems are being introduced and should be resourced as part of the change project.

14.16 Working with the Information Governance Division to respond to information rights requests. For example, data subject access requests and freedom of information requests.

Time commitment: Varies considerably depending on the number of requests and their scope and complexity.

14.17 Raise awareness in their school or professional service of information management good practice to support and guide colleagues to use information wisely and in accordance with relevant policies, procedures, and business rules. This may include: providing local information management induction sessions for new colleagues to supplement the mandatory University-wide online training; using awareness raising materials provided by the Information Governance Division to provide an annual refresher briefing to colleagues at a team meeting.

Time commitment: Approximately 1-7 hours each year.

14.18 Where a LIAM's remit includes structured information in line of business applications, the LIAM will also have responsibilities under the framework being developed by the Strategic Planning, Performance and Projects Directorate. These responsibilities are likely to include drafting data definitions, investigating data quality issues and recommending remedial action to the IAO.

POLICY

15. APPENDIX 4: COMPLIANCE WITH THE CODE OF PRACTICE ON RECORDS MANAGEMENT

Table 1 below maps the requirements of the FOISA section 61 Code of Practice on Records Management to the relevant sections of this Policy.

Table 2 maps the Model Records Management Plan issued under section 1 of the Public Records (Scotland) Act 2011 (which provides practical guidance on the development of records management programmes) to the Code of Practice on Records Management.

Code of Practice on Records Management requirements		**Information Governance & Records Management Policy**	
Ref	**Description**	**Ref**	**Description**
1	Organisation arrangements to support records management (Includes "Induction and other training")	2	Purpose
		5	Lines of responsibility
		7	Information and Records Management Programme
		7.8	Promote good records management practices
		8.2	Risk Management
2	Records management policy	2	Purpose
		5	Lines of responsibility
3	Keeping records to meet corporate requirements	7.9	Business rules
4	Record systems	7.11	Embed effective IG into all new and upgraded information systems
5	Storage and maintenance of records	7.12	Develop an information asset register
6	Security and access	7.14	Information security good practice
7	Disposal of records	7.11	Disposal arrangements
8	Records created in the course of collaborative working or through out-sourcing	7.15	Promote good IG practice when sharing information externally
9	Monitoring and reporting on records and information management	6	Monitoring and evaluation
		7.7	Establish a network of Local Information Asset Managers

Table 1

FOISA RM CoP requirements		**PRSA MRMP**	
Ref	**Description**	**Ref**	**Description**
1	Organisation arrangements to support records management	1	Senior management responsibility
		2	Records manager responsibility
2	Records management policy	3	Records management policy statement
3	Keeping records to meet corporate requirements	4	Business classification
		9	Data protection

FOISA RM CoP requirements		PRSA MRMP	
Ref	**Description**	**Ref**	**Description**
		12	Records management training for staff
4	Record systems	4	Business classification
		8	Information security
		9	Data protection
		11	Audit trail: Tracking and version control
		12	Records management training for staff
5	Storage and maintenance of records	4	Business classification
		9	Data protection
		10	Business continuity and vital records
		11	Audit trail: Tracking and version control
6	Security and access	8	Information security
		9	Data protection
7	Disposal of records	5	Retention schedules
		6	Destruction arrangements
		7	Archiving and transfer arrangements
		9	Data protection
8	Records created in the course of collaborative working or through out-sourcing	14	Shared information
		15	Public records created by third parties
9	Monitoring and reporting on records and information management	13	Assessment and review

Table 2

POLICY

16. APPENDIX 5: EQUALITY AND DATA PROTECTION IMPACT ASSESSMENTS

Responsibility for this assessment:	Anne Grzybowski Records Manager Information Governance Division Governance and Legal Services Telephone: 0131 451 4140 Email: InfoGov@hw.ac.uk
Date of assessment:	22 November 2021
Date for future review of policy/function:	When the Policy is next reviewed, which is five years from the date of approval or more frequently if required
Policy or process being assessed:	Information Governance and Records Management Policy
New or existing policy?	This assessment relates to the updates to an existing policy. This is the first time an equality impact assessment has been carried out for this policy

The Policy

1	Briefly describe the aims, objectives, and purpose of the policy, and any associated objectives of the policy.
	The aim of the Policy is for the University to be accountable for, and transparent about, its activities, by applying information governance principles to the management of its information assets (see section 3 of the Policy for details). The purpose of the Policy is to manage the University's information assets to: • Deliver the University's mission and strategic objectives • Meet legal, compliance and accountability obligations • Provide business continuity, maintain the University's corporate memory, and preserve the historical record (see section 2 of the Policy for details). The Policy sets out lines of accountability and responsibility and outlines an Information and Records Management Programme through which the Policy will be implemented.
2	Does the policy impact people?
	Yes. The University's information assets are created, received, and used by people, including people with protected characteristics. The format and design of those information assets can impact the extent to which they are accessible to different equality groups.

	Many of the University's information assets contain information about people. Those individuals are data subjects and have rights in relation to the information the University holds about them. The information we create and retain (or do not create and retain) provides the basis for the University's decision-making and its corporate memory. In the future it may also provide the basis for machine learning and the development of algorithms that may be used to automate or streamline decision making processes. Equalities groups are impacted by being under-represented in information assets. This has an impact on: • Whether services are designed fairly, or not • Whether decisions are fair and whether they have an adverse impact on under-documented demographics • The visibility of equalities groups in the historical record, and the extent to which individuals from those groups can see themselves represented in the University Museum and Archive
3	Who is intended to benefit from the policy and in what way?
	The Policy is intended to benefit: • All university stakeholders, by providing the information governance framework which will provide evidence of their rights and entitlements • Data subjects, by making the University accountable and transparent about its processing of personal data • University staff and service users, by providing the information governance framework that allows effective and efficient information handling to deliver timely and responsive services • University managers, by providing the framework to improve access to accurate information for decision-making • University staff, by providing the information governance framework which will allow them to account for their actions and decisions and demonstrate they have performed their duties appropriately • University staff, by establishing training and support to help them fulfil their existing information management responsibilities • Future generations, by enabling records of lasting value to be preserved and made accessible through the University Museum and Archive • Future generations, by reducing waste and making more effective and sustainable use of resources
4	Is any data available about the policy, e.g. feedback from users?
	The revised Policy was issued to all staff for consultation on 14 May 2021. The consultation remained open until 27 June and late responses were accepted until 11 July.
5	What outcomes are wanted from this policy?
	The Policy is intended to make the University accountable and transparent about its activities. Accountability and transparency are pre-requisites for building and

POLICY

	maintaining the trust of individuals and for designing and delivering equitable decisions and services. By embedding information governance principles in the way we manage university information, the Policy will facilitate the creation and maintenance of information assets that exclude as few individuals as possible.
6	What factors/forces could contribute/detract from the outcomes?
	The Information and Records Management Programme (see section 7 of the Policy) must be implemented, including: • Training and awareness raising that will help individuals to embed the information governance principles into their work • Developing business rules that take account of information accessibility issues and the importance of fully documenting and justifying information collection and retention requirements

Equality Impact Assessment

7	The Equality Act 2010 includes a requirement to give 'due regard' to the public sector equality duty (PSED) in all functions. There is a specific duty to assess the impact of proposed new or revised policies and practices against three needs of the general duty. Use this section to outline relevant issues.	
	Eliminate unlawful discrimination, harassment, and victimisation	The creation and maintenance of accurate, consistent, and inclusive records will help the University to assess the extent to which unlawful activities are taking place and which groups are affected. For example, the use of consistent definitions for different types of problem behaviour and accurate, effective record-keeping in relation to reported incidents allows the University to establish benchmarking, use comparators and conduct gap analysis.
	Advance equality of opportunity between people of different groups	Taking account of the needs of different equality groups at record creation stage and creating effective records consistently across the University, will help to meet the needs of different equality groups.
	Foster good relations between people of different groups	The Policy specifically aligns with the University's strategic goal "Building Flourishing Communities" and the University's values to belong and collaborate (see section 2.3 of the Policy). Transparent and accountable record-keeping is a fundamental building block to build flourishing communities which foster good relations between people of different groups.
8	Do you have any concerns that the policy could have a differential impact on any of the Protected Characteristic groups? Detail any relevant information.	

	It may be beneficial to give particular consideration to the Protected Characteristic groups in your impact assessment. The Protected Characteristics covered by the Equality Act 2010 are: Age, Disability, Race, Religion and Belief (including no belief), Sex, Sexual Orientation, Pregnancy and Maternity, Gender Reassignment, Marriage and Civil Partnership.
	The Policy applies to everyone working on behalf of the University, including employees, casual workers, contractors, agents, and those with an honorary or voluntary role, whenever they are carrying out work for the University that involves (or ought to involve) the creation, receipt, or use of information assets (see section 4 of the Policy). The people to whom the Policy applies include people with protected characteristics. Without this Policy and its implementation, it is possible that traditional information management practices could have a differential impact on: • People with disabilities – Some people use assistive technologies to create and use information. Some information formats and formatting are less accessible to some people. Information which lacks metadata, or which applies metadata inconsistently is less accessible to some people. • Younger people and females – Traditionally record-keeping responsibilities have been assigned to junior, often female, staff. This Policy identifies the record-keeping responsibilities that all staff have. • Gender reassignment – The importance of accurate record-keeping means that University records should reflect an individual's gender identity. We recognise that there may be a differential impact on equality groups whose first language is not English, as most university information assets are in English. We also recognise that English is the primary language in which the University operates. These groups may find that idioms and culturally specific language are less accessible. This impact can be mitigated through guidance and training that reminds colleagues to avoid ambiguity and use language that is appropriate to the audience. We do not expect this Policy to have a specific differential impact on Religion and Belief, Sexual Orientation, Pregnancy and Maternity, Marriage and Civil Partnership. The Policy is intended to prevent negative differential impacts by maintaining the information needed to comply with the University's equalities duties and data protection obligations.
9	What are the risks associated with the policy in relation to differential impact?
	If the Policy is not consistently implemented, some equalities groups may not be visible in the University's information assets.
10	Could the differential impact identified in 6-11 amount to there being the potential for adverse impact in this policy? If no, outline why and go to question 12.

POLICY

	No. The Policy is intended to provide the basis to counter differential impacts resulting from poor information governance.
11	Can this adverse impact be justified on the grounds of promoting equality of opportunity for one group? Or any other reason.
	N/A
12	Demonstrate how you have involved stakeholders in the equality impact assessment.
	The policy consultation process and the responses received have informed the drafting of this equality impact assessment. This equality impact assessment is included as an appendix to the Policy so that stakeholder representatives can comment on it as part of the next stage of Policy consultation and approval.

Data Protection Impact Assessment: Screening questionnaire

13	Does implementation of the policy or procedure necessitate processing:	
	Information about people who can be identified from that information or in combination with other information ('personal data')	Yes. The Policy applies to information assets that contain personal data.
	Personal data about: racial or ethnic origin; political opinions; religious of philosophical beliefs; trade union membership; physical or mental health; sex life or sexual orientation; proven or alleged offences, including criminal convictions ('special category personal data')	Yes. The Policy applies to information assets that contain special category personal data.
	Confidential information that is not personal data	Yes. The Policy applies to information assets that contain confidential information.
14	Does implementation of the policy or procedure involve:	
	Transfers of personal data outside the UK to organisations that are not members of the Heriot-Watt University Group?	No. The Policy supports compliance with the Data Protection Policy which governs transfers of personal data outside the UK to organisations that are not members of the University Group.

POLICY

Collecting any new categories of personal data about individuals that we don't already collect about them?	No. The Policy supports compliance with the Data Protection Policy which governs the collection of new categories of personal data.
A change to the nature, scope, context, or purpose of our processing and/or the use of information about individuals	No. The Policy supports compliance with the Data Protection Policy which governs changes to the University's processing of personal data.
Compelling individuals to provide personal data about themselves that is not strictly necessary?	No. The Policy supports compliance with the Data Protection Policy which governs the collection of personal data.
Disclosing personal data or other confidential information about individuals to people or organisations who have not previously had routine access to it?	No. The Policy supports compliance with the Data Protection Policy which governs the disclosure of personal data.
Contacting individuals in ways that they may find intrusive?	No. The Policy supports compliance with the Data Protection Policy which governs the University's processing of personal data.
Sharing personal data about individuals without their consent where there isn't a statutory reason to do so?	No. The Policy supports compliance with the Data Protection Policy which governs the sharing of personal data.
A high risk to individuals which would make a data protection impact assessment mandatory?	No. The Policy supports compliance with the Data Protection Policy.