Information Governance and Records Management Policy

March 2014

POLICY

Approving authority:	Secretary's Board
Consultation via:	Secretary's Board Information Governance and Security Group
Approval date:	4 March 2014
Effective date:	March 2014
Review period:	Five years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Heritage and Information Governance

HERIOT-WATT UNIVERSITY
INFORMATION GOVERNANCE AND RECORDS MANAGEMENT POLICY
CONTENTS

POLICY

1. INTRODUCTION

Information is a vital University asset. The creation of a *single point of truth* is one of the key enabling strategies on which the University Strategy depends. To achieve this, it is necessary to agree and apply policies and procedures to promote the effective management of University information in all formats throughout its lifecycle, in order to provide accurate and reliable records of actions and decisions and meet operational, legal and evidential requirements.

Records created in the course of University business belong to the University, rather than the individuals that create or use them. However, all staff and other providers of University services have defined and shared responsibilities for managing records.

This policy sets set out a framework of governance and accountability for the management of University records in all formats within the wider University information governance and security framework.

2. PURPOSE

Sound and effective information governance systems are vital to the University's mission to create and exchange knowledge for the benefit of society.

Through this policy the University aims to create and maintain accurate, reliable and well managed records that it relies upon to

- Provide a high quality service for our students and keep an accurate account of their University journey from application to academic achievement and alumni relations
- Support the delivery of our learning and teaching strategy
- Document, protect and share our academic research
- Inform our choices, actions and decisions and to provide accountable evidence of these
- Work collaboratively and effectively with colleagues, students and partners worldwide
- Give students, staff and stakeholders confidence that we keep their confidential information secure
- Make the most effective use of our resources and demonstrate value for money
- Manage risks, defend our interests and strengthen the University's reputation

POLICY

- Ensure our business continuity
- Meet our statutory obligations
- Protect our corporate memory

3. OBJECTIVES

This policy and its supporting procedures aim to support the creation and management of University records and records systems that

- Are accurate, reliable and comprehensive and avoid unnecessary duplication, forming a single point of truth
- Support effective and efficient business processes, service delivery and decision-making
- Can be retrieved promptly by those that need to use them
- Are protected against unauthorised access, disclosure, alteration or destruction
- Are managed cost effectively, in the medium most appropriate for the task they perform and are retained only as long as needed
- Support resilience and business continuity
- Remain accessible for as long as they are required
- Enable the University to meet its audit and regulatory obligations under financial, charity and information laws, including Data Protection and Freedom of Information legislation, in all the jurisdictions in which it operates
- When no longer in current use will be stored cheaply, retrieved promptly, reviewed and disposed of securely in accordance with a defined policy and approval process
- Where worthy of permanent preservation as archives are identified as early as possible and preserved in the University Archive

This policy and its supporting procedures and guidance have been scoped to meet the requirements of the Scottish Government Code of Practice on Records Management, issued under Section 61 of the Freedom of Information (Scotland Act) 2002, which set out record keeping responsibilities for all Scottish public authorities including the University.

POLICY

4. SCOPE

4.1 What information is included in the Policy

This policy applies to all records created, received and maintained by University staff, contractors and other University users in the course of University business, in all formats, of any age.

4.2 Who is affected by the Policy

The policy applies to all employees and contractors of the University and anyone else working in an honorary or voluntary role for the University, who may create, receive or have access to University records.

4.3 Where the Policy applies

The policy applies to all locations in which University records are created, received and used, including home use.

As the University operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the policy shall include such overseas campuses and international activities and shall pay due regard to non UK legislation that might be applicable.

5. LINES OF RESPONSIBILITY

All staff, contactors and others with University record keeping responsibilities are responsible for

- maintaining accurate and reliable records in line with their roles and responsibilities
- ensuring that these records are backed up onto University IT systems
- applying good housekeeping principles; by using naming conventions and version control, following filing procedures and saving relevant emails to shared information systems to ensure that in their absence, other colleagues with a business or legal need to do so can readily find the right information
- following the University information security policies and procedures to protect records containing personal data and other confidential information from unauthorised access
- working with their managers and colleagues to apply the records retention policies relevant to their work; so that records are kept locally only as long as required and then securely destroyed or transferred by arrangement with HIG for longer term storage or archival preservation
- undertaking relevant training and awareness activities provided by the University to support compliance with this policy
- arranging orderly handover of all records that they hold to their

POLICY

manager before leaving the University

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

5.2 **The Director of Governance and Legal Services** has senior management responsibility for information governance

5.3 **The Head of Heritage and Information Governance** (HIG) is responsible for recommending information governance and records management strategy and policies to the Director of Governance and Legal Services and leading the information governance programme, promoting good practice, monitoring compliance and recommending revisions to these policies in line with business need, legal requirements and professional standards.

5.4 **All Heads of Schools, Institutes and Professional Services** are responsible for implementing the policy within their business areas, and for adherence by their staff. This includes

- Assigning generic and specific responsibilities for information governance and records management
- Liaising with Heritage and Information Governance to agree and apply records retention policies, transfer and disposal arrangements for their areas of responsibility
- Managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such confidential information as is necessary for them to fulfil their duties.
- Ensuring that all staff in their business areas undertake relevant training provided by the University and are aware of their accountability for information governance
- Ensuring that staff responsible for any locally managed IT services liaise with University Information Services staff and HIG to apply information governance, records management and archive processes and controls

5.5 **The Director of Information Services** is responsible for

- Working in partnership with HIG and the records creators to plan and develop central IT systems to meet the University's information governance and records management requirements.

- Maintaining University IT systems to ensure that records held within them can remain authentic, reliable and usable throughout any system change, including format conversion, migration between hardware and operating systems or specific software applications, for as long as they need to be retained

- Agreeing an exit strategy for each IT system that holds university records, such as finance, research staff or student records, with the

POLICY

responsible officers and HIG so that retention and archiving requirements can be identified and met

- Developing and implementing digital preservation procedures for the long term preservation of and access to records of archival value

5.6 **The Director of Human Resources** is responsible for reviewing relevant human resources policies and procedures, in order to support managers and staff in understanding and discharging their responsibilities for information governance and records management through the recruitment, induction, training, promotion, discipline and leaver management processes.

5.7 **The Academic Registrar and Deputy Secretary** is responsible for reviewing relevant student administration policies and procedures to integrate with the information security management system and for oversight of the management of student records and associated personal data across the University.

6. MONITORING AND EVALUATION

6.1 The Head of Heritage and Information Governance will monitor the implementation of this policy and its underpinning programme, report on progress to the Director of Governance and Legal Services and consider measures to enhance effective information management and respond to developments in the regulatory and risk environment.

The Head of Heritage and Information Governance will liaise with the Director of Information Services and the Head of Risk and Audit to ensure that information governance risks are captured on the operational risk register and that Schools, Institutes and Professional Service record relevant risks on their local registers.

6.2 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.

The Information Governance and Security Group will review information governance and security related policies and procedures, monitoring the effectiveness of controls and recommending measures to ensure the confidentiality, integrity and availability of University records and information assets.

The Strategic Information Systems Group promotes coherence and collaboration in planning and development of information and IT systems to support the University's business and evidential needs and identifies opportunities to strengthen information governance and reduce duplication of information in shadow and complementary systems

POLICY

The Collections Committee has oversight of the stewardship and development of the University Museum and Archive Collections. In this capacity the Committee will monitor the effectiveness of information governance policies, procedures and measures and recommend any changes necessary to achieve the University's objective to preserve records of archival value as the corporate memory; to record and celebrate student experience, academic achievement and University life.

7. IMPLEMENTATION

7.1 To achieve its objectives and contribute to the wider framework of effective information governance this policy is underpinned by a continuous and incremental records management programme. Led by Heritage and Information Governance working collaboratively in partnership with Information Services, Schools and Professional Services, this programme is designed to support the effective management of University records throughout their lifecycle. Some elements of this programme also fall within the information security management programme developed under the auspices of the Information Security Policy Framework.

This policy is supported by detailed records retention schedules, setting out retention and destruction policies for records of all University activities, based on higher education sector best practice recommendations by the Joint Information Systems Committee (JISC). Heritage and Information Governance staff will engage with Heads of Schools and Professional Services to agree and apply records retention schedules and archiving arrangements for their areas of responsibility.

Where required, this policy is supplemented by more detailed policies for specific categories of record, such as Student Records, and to meet the complex challenges of digital preservation

The core elements of the records management programme are as follows:

7.2 Creating and managing electronic and paper records:

- Establish an information governance framework for each campus to agree roles and responsibilities, assist in identification of the University's information needs, reduce duplication and shadow systems
- Input into the specification and development of information systems so that they are fit for purpose and provide authentic and reliable records of actions and decisions
- Apply “privacy by design” principles when developing and managing information systems containing personal data
- Develop best practice guidance on organising, filing, naming and version control of records so that the "single point of truth" can be readily identified and retrieved
- Recommend standards for creation and management of electronic records required for evidential purposes
- Identify and protect records that are vital for business continuity

POLICY

- Establish an electronic repository for all records that we need to keep in order to protect our interests and reputation and comply with the law

7.3 Mitigating information security risk by recommending physical, personnel, governance and technology controls to maintain

- Confidentiality: protecting information from unauthorised access and disclosure
- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion
- Availability: ensuring that information and associated services are available to authorised users when required

7.4 Complying with access to information and privacy laws and other regulatory requirements

- Proactive publication of University information
- Facilitate direct access to information and datasets and appropriate data sharing agreements
- Respond to requests for information in a fair, friendly and timely fashion
- Audit the personal data that we hold and ensure that it is managed in accordance with the rights of the individual
- Protect confidential information by appropriate use of exemptions to the right of access

7.5 Applying records retention and destruction policies

- Agree and monitor the implementation of records retention, transfer and disposal schedules so that each School and Professional Service retains records locally only as long as needed
- Manage the provision of appropriate storage for electronic and paper records that need to be kept for a limited time
- Specify and monitor the implementation of procedures for secure destruction of time-expired records in all formats

7.6 Selecting records for permanent preservation as archives

- Identify records worthy of permanent preservation as early as possible in their lifecycle
- Agree the formats required for preservation and contextual metadata to be captured
- Plan and manage their orderly and timeous transfer into the University Archive for accession and management as part of the University Collections

POLICY

7.7 Awareness raising, training and user engagement: for all staff, and members of the University community

- Induction
- Generic awareness raising
- Role specific e.g. researchers, student records administrators
- Leaver management

7.8 Develop and implement a University digital preservation programme for

- Corporate archives,
- Research data,
- Still and moving images and audio-visual recordings

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1 University Policies and procedures

This policy should be read in conjunction with all other University information governance and management 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 http://www.hw.ac.uk/staff/policies-governance/procedures/information-records.htm

These include

Information Security Policy Framework and its constituent policies and procedures

IT and Communications Acceptable Use Policy

Student Records Management Policy

Data Protection Policy

8.2 Legal Requirements and external standards

Effective information governance is essential for compliance with U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

Legislation that places specific information governance and record keeping obligations on organisations includes, but is not limited to:

Computer Misuse Act 1990
Data Protection Act 1998
Environmental Information (Scotland) Regulations 2004
Freedom of Information (Scotland) Act 2002 and its Codes of Practice on Functions of Public Authorities

POLICY

http://www.scotland.gov.uk/Resource/Doc/933/0109425.pdf
and Records Management
http://www.scotland.gov.uk/Resource/Doc/933/0124124.pdf

Privacy and Electronic Communications Regulations 2003
Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Scotland) Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

All current UK Legislation is published at http://www.legislation.gov.uk/

Heritage and Information Governance staff can advise on specific legal and regulatory requirements affecting records and information management.

Records retention polices are based on the following higher education standard of good practice:

JISC Infonet: HEI records retention policies and business classification scheme
http://bcs.jiscinfonet.ac.uk/he/

This policy also supports compliance with the following international standards:

BS ISO 27001 Information Security Management.
BS ISO 15489 Information and documentation. Records Management

9. DEFINITIONS

Information	The definition of 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.
Record	A Record is information in any format that has been generated or received by the University in the course of its activities which must be retained by the University as evidence of its actions and decisions for operational or legal purposes
Archives	Records which have been created or received by the University in the course of its activities and functions and selected for permanent preservation for their historical or evidential value, by HIG in

POLICY

consultation with the records creators.

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.

Records management

Records management is a key component of information governance. It supports the effective management of information of evidential value throughout its lifecycle from planned creation and active use to controlled and accountable destruction or archival preservation.

Confidential information

The definition of confidential information can be summarised as:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent.
- Any other Information that would prejudice the University's or another party's interests if it were disclosed without authorisation.

A more detailed definition can be found in the **Policy for secure use of confidential information on portable media**

Information Security Management System

"That part of the overall management system based on a business risk approach to establish, implement operate, monitor review maintain and improve information security. The management system includes organisational structure, polices, planning activities, responsibilities, practices, procedures, processes and resources."
BS ISO/IEC 27001: Information Security

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of records management and information governance contact:

Ann Jones
Head of Heritage and Information Governance

Brian Kelvin
Records Manager
Heritage and Information Governance
Governance and Legal Services

Telephone: 0131 451 3274/3219
Email: foi@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V4 21/02/2014	4 March 2014	Secretary's Board	Revisions to take account, legal, technological, business and risk environment; minor amendments to Lines of Responsibility following consultation

POLICY