

Information Security Policy Framework

January 2019

Approving authority:	University Executive
Consultation via:	Professional Services Leadership Board, Global Information Governance and Data Protection Group
Approval date:	29 January 2019
Effective date:	29 January 2019
Review period:	Five years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Information Governance, Information Services
Territorial Scope	University Group, Global

**HERIOT-WATT UNIVERSITY
INFORMATION SECURITY POLICY FRAMEWORK
CONTENTS**

Section		Page
1	<u>Introduction</u>	3
2	<u>Purpose</u>	3
3	<u>Objectives</u>	3
4	<u>Scope</u>	4
5	<u>Lines of responsibility</u>	5
6	<u>Monitoring and Evaluation</u>	6
7	<u>Implementation</u>	7
8	<u>Related Policies, procedures and further reference</u>	8
9	<u>Definitions</u>	9
10	<u>Further help and advice</u>	10
11	<u>Policy Version and History</u>	10

1. INTRODUCTION

This policy sets out a framework of governance and accountability for information security management across the University Group. It forms the basis of the University Information **Security Management System (ISMS)**. This incorporates all policies and procedures that are required to protect University information by maintaining

- **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 whenever and wherever required
- **Resilience** of processing systems and services: the ability to defend against and mitigate the impact of a physical or technical incident and restore the availability and access to information in a timely manner

This policy framework aims to develop a positive culture of information security throughout the University.

2. PURPOSE

Heriot-Watt University relies on the effective management and flow of information to enable staff to communicate and work effectively on its business worldwide. The need to access information must be balanced with appropriate and proportionate measures to avoid the loss or unauthorised disclosure of confidential information.

The purpose of this policy is to establish an effective Information Security Management System to

- Ensure our business continuity
- Protect our intellectual property rights, financial interests and competitive edge
- Safeguard the interests and privacy of our students, staff and stakeholders and retain their trust
- Comply with the law and defend ourselves against legal action
- Maintain our reputation

3. OBJECTIVES

This policy framework sets out the University's senior management commitment to information security and establishes a framework of governance, responsibility and accountability for information security management across the University Group. The policy applies to all information created or received in the course of University business.

This policy framework forms the basis of the University Information Security Management System (ISMS) of related policies and procedures, based on the International Standard BS EN ISO/IEC 27001:2017, taking a risk based, proportionate approach to embed appropriate levels of information security controls in the University's business functions and processes.

- 3.1** This policy framework sets out generic and specific lines of responsibility for information management across the University.

All members of the University community have a responsibility to protect all confidential information to which they may have access in the course of their work.

Within this policy framework, Heads of Schools, Chief Operating Officers, Directors of Professional Services, managers and relevant professional specialists are responsible for working together with information users to develop, implement, monitor and review the components of the information security management system.

- 3.2** The University takes its responsibilities for information security very seriously.

Any user who breaches information security policy may be liable to disciplinary action and may also be breaking criminal or civil law. Breaches of the policy which place the University at serious financial, commercial or reputational risk or actual loss may be considered as gross misconduct offences, for which dismissal may be an outcome.

4. SCOPE

4.1 What information is included in the Policy framework

This policy framework applies to all information created or received in the course of University business in all formats, of any age. This policy applies to information held or transmitted in paper and electronic formats or communicated verbally in conversation or over the telephone.

4.2 Who is affected by the Policy Framework

The policy framework applies to all users of University information. Users include all employees and students of the University, all contractors, suppliers, University partners and external researchers and visitors who may have access to University information.

4.3 Where the Policy Framework applies

The policy framework applies to all locations from which University information is accessed including home use.

As the University Group operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the policy framework and the Global Information

Governance and Data Protection Group 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

5.1 All users of University information are responsible for

- Undertaking relevant training and awareness activities provided by the University to support compliance with this policy
- Taking all necessary steps to ensure that no breaches of information security result from their actions.
- Reporting all suspected information security breaches or incidents promptly to ITHelp@hw.ac.uk so that appropriate action can be taken to minimise harm.

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

5.3 The Director of Governance and Legal Services has senior management responsibility for the information security management and for providing proactive leadership to instil a culture of information security within the University through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

5.4 The Director of Information Services is responsible for recommending IT security policies, maintaining controls to ensure that centrally managed IT systems and services take account of information security risks and are integrated into the information security management system, in line with cybersecurity standards, and for promoting good practice in IT security among relevant staff.

5.5 The Head of Information Governance and Data Protection Officer is responsible for recommending information security policy and ISMS to the Director of Governance and Legal Services, leading on wider information governance strategy, policies and procedures and for recommending any University policies necessary to comply with data protection law or other regulations affecting the management of information and records.

5.6 All Heads of Schools, Chief Operating Officers, 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 security management

- Managing access rights for information assets and systems to ensure that employees, contractors, agents and other users have access only to such confidential information as is necessary for them to fulfil their duties.
- Ensuring that all colleagues in their business areas undertake relevant training provided by the University and are aware of their accountability for information security
- Ensuring that staff responsible for any locally managed IT services liaise with University Information Services staff to put in place equivalent IT security controls

5.6 The Global Director of Human Resources Development is responsible for reviewing relevant human resources policies and procedures to integrate with the information security management system, in order to support managers and staff in understanding and discharging their responsibilities for maintaining information security, through the recruitment, induction, training, promotion, discipline and leaver management processes.

5.7 The Academic Registrar 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.

5.8 The Head of Assurance Services is responsible for ensuring that Information Security controls are integrated within the risk, business continuity management and audit programmes and for liaising with insurers to ensure that the ISMS meets insurance requirements.

5.9 The Director of Safeguarding Services is responsible for ensuring that controls to manage the physical security of the University takes account of relevant information security risks and are integrated into the information security management system.

5.10 The Global Information Governance and Data Protection Group is responsible for reviewing the information security related policies and procedures that comprise the ISMS, monitoring compliance with the ISMS, reviewing incidents and recommending actions where necessary to strengthen information security controls. The Director of Governance and Legal Services chairs the group. Its membership will include the Head of Information Governance and Data Protection Officer, the Director of Information Services and representatives of all of the senior stakeholders with responsibilities for information security, as set out in the Terms of Reference for the Group.

6. MONITORING AND EVALUATION

The Head of Information Governance and Data Protection Officer will monitor new and on-going information security risks and recommend

updates to the information governance strategic risk register, reporting these promptly as required to the Director of Governance and Legal Services and the Head of Assurance Services. The Head of Information Governance and Data Protection Officer will liaise with the Director of Information Services and the Head of Assurance Services to ensure that IT security risks are captured on the register and that Schools and Professional Service record relevant information security risks on their local registers.

- 6.1** The Chair of the Global Information Governance and Data Protection Group and the Data Protection Officer will make an annual report to the Risk and Project Management Strategy Group on compliance with the ISMS, recommending any actions needed to address risks and issues, for inclusion in the Audit and Risk Committee's annual report on risk management control to Court. The Chair is responsible for escalating major risks arising from a breach of information security, or other major issues that affect strategic and operational risks, promptly to the Risk and Project Management Strategy Group and the Secretary of the University. The Chair will report as necessary to the Professional Services Leadership Board as part of a wider communications strategy to promote a culture of responsible information security management across the University.

The Head of Information Governance and Data Protection Officer is responsible for reporting any information security issues with data protection compliance implications to the Secretary of the University and for liaising with the Information Commissioner's Office or the relevant Supervisory Authority in relation to data protection compliance matters.

The Director of Governance and Legal Services is responsible for meeting any reporting requirements of other external regulatory bodies.

- 6.2** As part of the University's internal audit programme, the Audit and Risk Committee will instruct the University's Internal Auditors to audit the management of information security risks and compliance with relevant controls, as required.

7. IMPLEMENTATION

This policy is implemented through the development, implementation, monitoring and review of the component parts of the information security management systems.

These include

- Heads of Schools and Directors of Professional Services undertake information risk assessments to identify and protect confidential and business critical information assets and IT systems
- Coordination of effort between relevant Heads of Service and professional specialists to integrate, IT, physical security, people,

- information governance, risk management and business continuity to deliver effective and proportional information security controls
- Review and refresh of all relevant policies and procedures
 - Designation of information governance coordinators for each area
 - Generic and role specific training and awareness
 - Embedding information governance requirements into procurement and project planning
 - Information security incident management policies and procedures
 - Business continuity management
 - Monitoring compliance and reviewing controls to meet business needs

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1. University Policies and procedures

This policy provides the framework for an interconnected set of [University Information Governance and IT Policies](#) and procedures. These aim to develop a positive culture of information governance throughout the University through the development of a holistic Information Security Management System (ISMS) to protect University information by maintaining its confidentiality, integrity, availability and resilience.

This policy framework should be read in conjunction with all other University information management policies, which are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the University's business needs and legal obligations. Relevant polices are published on the University website at [Our policies | Heriot-Watt University](#)

Managers of staff whose roles do not require University IT access are responsible for briefing their staff on their responsibilities in relation to all polices that affect their work.

8.2 Legal Requirements and external standards

Effective information security controls are 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 security and record keeping obligations on organisations includes, but is not limited to:

Computer Misuse Act 1990
Data Protection Act 2018
European Union General Data Protection Regulation (GDPR)
Environmental Information (Scotland) Regulations 2004
Freedom of Information (Scotland) Act 2002
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 <https://www.legislation.gov.uk/>

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

This policy also maps to BS ISO 27001 Information Security 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.

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 University [Information Security Classification Scheme](#)

Information Security Management System

"An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for

establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks." - BS EN ISO/IEC 27000:2017

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of information security contact:
 Information Governance
 Telephone: 0131 451 3216/3274/3219
 Email: Infogov@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V12.1 22/11/2018	29 January 2019	University Executive	Roles and remit updated for review by GIGDPG and onward approval; territorial scope added to title page. Update of Version 11 approved September 2013