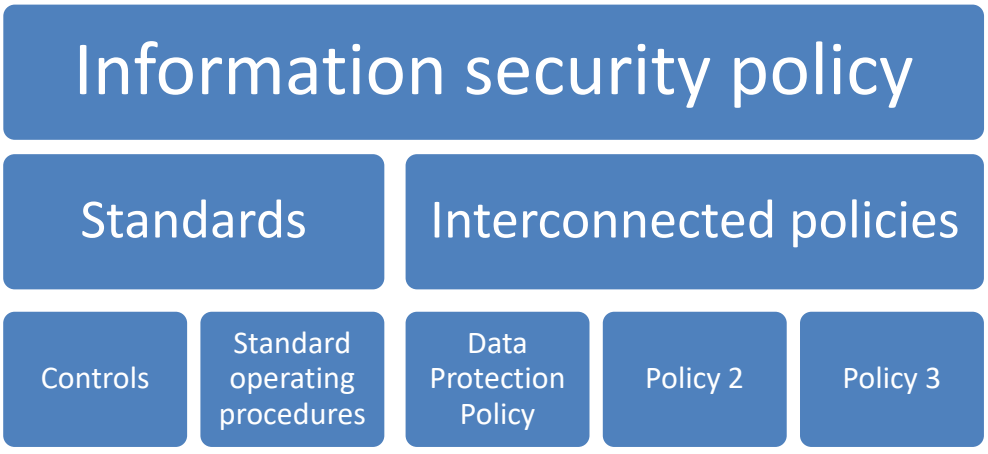
Information Security Policy

May 2023

Approving authority:	University Executive
Consultation via:	Global Operations Executive, Global Information Governance and Data Protection Committee, CJNCC
Approval date:	24 May 2023
Effective date:	24 May 2023
Review period:	Five years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Information Services Information Governance
Territorial Scope	Global University and Heriot-Watt Group

HERIOT-WATT UNIVERSITY
INFORMATION SECURITY POLICY
CONTENTS

1.	**INTRODUCTION**
	This policy sets out the University's approach to information security risk management and provides a structure of governance and accountability for information security management across the Global University and Heriot-Watt Group. All members of the University have responsibilities under this policy. The policy forms an integral part of the University Information Security **Framework.** This Framework incorporates this policy and the associated policies, standards and procedures that are required to protect University information assets and technology services 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; this includes non-repudiation, the ability to prove that an action was taken ▪ **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 The Framework provides a flexible and effective platform to achieve the University's information security objectives. The Framework is shown below, 
	The Framework aims to develop a positive "information security aware" culture throughout the Global University and affirms that information security is everyone's responsibility.

POLICY

2.	**PURPOSE**
	As a globally connected University Heriot-Watt relies on the effective management and flow of information to support its mission to create and share knowledge for public benefit and achieve its strategic goals. The need to access information must be balanced with appropriate and proportionate measures to protect our information assets and systems and avoid the loss, compromise or unauthorised disclosure of personal data and other confidential information. The purpose of this policy is to set out roles and responsibilities so that each member of the University understands their duty to help deliver and maintain an effective Information Security Management Framework.
3.	**OBJECTIVES**
	The Policy and Framework are designed to • Protect the University's own information assets and technology services and assets being processed or held by the University on behalf of other parties by identifying, managing and mitigating information security threats and risks. • Define security requirements that are effective, sustainable and measurable and achieve the appropriate balance of usability and security. • Identify, contain, remediate and investigate information security incidents and apply lessons learned to maintain and assist in improving the University's information security risk posture. • Develop an informed information security approach that takes account of the operational requirements for all areas of the University, including teaching, research, students and professional services • Assist in the compliance of contractual, legal or regulatory obligations. • Provide assurance to the governing body and internal and external stakeholders that the University has a robust control environment in place to protect information assets through an effective information security management system.

POLICY

4.	**POLICY STATEMENT**
4.1 4.2	All members of the University and all other users of University information and technology systems have a duty to protect the information and systems that they access and use for study and work and to comply with this Policy and Framework. Employees and contingent workers, including casual workers, contractors, agents, members of the governing body and people with an honorary or voluntary role have specific duties to implement the relevant elements of the Framework in line with their assigned roles and responsibilities.
5.0	**SCOPE**
5.1	**What is included in the Policy** This Policy applies to • All information and information assets created or received in the course of University business in relation to any University function in all formats, of any age • Information held or transmitted in paper and electronic formats or communicated verbally in conversation or over the telephone • Technologies or services used to access or process University information assets whether provided directly by the University or on its behalf by external suppliers and contractors. • Information assets processed in relation to any University function, including by, for, on behalf of, or with, external parties. • Information assets that are stored by the University or an external service provider on behalf of the University • Information that is created or transferred from and/or to the University for any functional purpose. • Any information that the University is storing, curating or using on behalf of any other party • Internal and/or external processes that are used to process, transfer or store University information
5.2	**Who is affected by the Policy** The Policy applies to all members of the University and other users of University information and technology systems. Users include all employees, other contingent workers, members of the governing body,

POLICY

	students and alumni of the University, all contractors, suppliers, University partners and external researchers and visitors who may have access to University information assets and technology from any location and by any means.
5.3	**Where the Policy applies** The Policy applies to all locations from which University information is accessed including home use. As the University and Heriot-Watt Group operate globally through its campuses in the United Kingdom, Dubai and Malaysia and through arrangements with partners in other jurisdictions the remit of this Policy includes all our campuses and activities and shall pay due regard to applicable legislation in each relevant country.
6.	**LINES OF RESPONSIBILITY**
6.1	**All users of University information, including members of the governing body, employees, contingent workers and students, are** responsible for protecting the confidentiality, integrity, availability and resilience of information and associated systems to which they may have access in the course of their work or study. • Complying with this Policy and all the standards, policies and procedures within the Framework that are relevant to their roles • Undertaking relevant training and awareness activities provided by the University to support compliance with this policy, in line with their roles and duties • Taking all necessary steps to protect University information and technology to ensure that no breaches of information security result from their actions • Reporting all suspected information security breaches or incidents immediately to IS Help so that appropriate action can be taken to minimise harm The University takes its responsibilities for information security very seriously. This Policy and Framework aim to build a positive culture of information security in which all members of the University feel confident to report security concerns or data breaches promptly without fear of retribution. It is then possible to work collaboratively to contain and mitigate the incident. As a university we always wish to learn from experience and seek opportunities, where practical, to reduce the risk of repetition. However, any user who deliberately or negligently breaches the measures set out in the Information Security Policy Framework may be

POLICY

	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 incur appropriate disciplinary sanctions for which dismissal or expulsion (as applicable) may be an outcome.
6.2	**Employees and contingent workers** are responsible for implementing the controls set out in the Framework as applicable to their roles and duties.
6.3	**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.
6.4	**The Global Director of Information Services** as the strategic risk owner for cyber security, has overall responsibility for this Policy and Framework, for recommending IT and Cyber security standards, procedures and controls, maintaining controls to ensure that technology systems and services take account of information security risks and are integrated into the information security management Framework,
6.5	**The Global Director of Governance and Legal Services** as the strategic risk owner for information governance has senior management responsibility for the information governance management
6.6	**Information Governance and Information Services are** responsible for collaboratively recommending the organisational and technical information security measures and controls that comprise the Framework, in consultation with relevant stakeholders, developing and maintaining the Framework, reviewing its effectiveness, and recommending enhancements in line with legal and business requirements, good practice and the threat environment.
6.7	**All Members of the University Executive** are responsible for approving this policy and are accountable for monitoring the effectiveness of the policy and the wider Information Security Framework that the policy supports.

POLICY

6.8	**All members of the Global Operational Executive are** responsible for implementing the policy within their business areas, and for adherence by their managers and staff. This includes ▪ Assigning generic and specific responsibilities for information security management to Information Asset Owners and Local Information Asset Managers within their business areas ▪ 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
6.8	**Information Asset Owners and Local Information Asset Managers** are responsible for maintaining the security of the systems and information assets for which they have assigned duties of stewardship, in line with their roles and responsibilities under the Framework and the Information Governance and Records Management Policy.
6.9	**The Global Information Governance and Data Protection Committee** is responsible for oversight of the information security related policies and procedures that comprise the Framework, monitoring compliance with the Framework, reviewing incidents and recommending actions where necessary to strengthen information security controls. The Committee reports to the University Executive and the Audit and Risk Committee of Court.
7.	**MONITORING AND EVALUATION**
7.1	Information Services and Information Governance are jointly responsible for reviewing this Policy and the Framework on a periodic basis to ensure they remain accurate, relevant and fit for purpose. They will report on relevant metrics, such as incidents and training activities, and recommend Policy and Framework changes to the Global Information Governance and Data Protection Committee.
8.	**IMPLEMENTATION**
	This policy is implemented through the development, implementation, monitoring and review of the component parts of the Framework and the design and delivery of appropriate training and awareness programmes.

POLICY

9.	**RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE**	
9.1.	**University Policies and procedures** This policy forms part of an interconnected Information Security Framework. This policy should be read in conjunction with the Framework all other University **Information Governance and IT Policies,** which are reviewed and updated as necessary 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 relevant polices that affect their work.	
9.2	**Legal Requirements and external standards** Effective information security controls are essential for compliance with UK and Scottish law and other relevant law in all jurisdictions in which the University operates. Information Governance staff can advise on specific legal and regulatory requirements affecting records and information management.	
10.	**DEFINITIONS**	
	Contingent worker	A person who does work for the University and is not directly employed on the payroll (i.e., does not receive a University payslip). Examples include but are not confined to casual worker, consultant, someone employed via a temping agency, an Adjunct Professor, Professor Emeritus, Visiting Scholar, a student on a work experience placement or a volunteer.
	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

POLICY

		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 Framework	The Framework, sometimes called an Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by the University in the pursuit of protecting its information assets and associated technology systems. The Framework is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives. It is based upon a risk assessment and the organisation's risk acceptance levels designed to effectively treat and manage risks. This definition is based on that for an ISMS in BS EN ISO/IEC 27000:2017
	Members of the University	All students and alumni, members of the governing body, Court, and its committees, employees and contingent workers including holders of honorary, visiting and emeritus titles of the University. Further details are set out in Article 1.2 of the Charter of the University and Ordinance A2: Members of the University
	University and Heriot-Watt Group	The University and its associated entities, including Heriot-Watt University Malaysia, Heriot-Watt Trading Ltd and others as stated

POLICY

		in Ordinance A1: Definitions and Interpretation

POLICY

11. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of information security contact:

Information Services Telephone +44 (0)131 451 4045 https://hwu.topdesk.net/ Email: ISHelp@hw.ac.uk	Information Governance Telephone: +44 (0)131 451 3216/3274/3219 Email: Infogov@hw.ac.uk

12. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V14.02	24/05/2023	University Executive	Update of policy (V12.1, approved 19/01/2019) revised in parallel with development of Framework, Roles and Responsibilities, Standards and Procedures.

POLICY