Data Protection Policy

June 2014

Approving authority:	Court
Consultation via:	Audit and Risk Committee, University Executive, Secretary's Board, Information Governance and Security Group
Approval date:	23 June 2014
Effective date:	23 June 2014
Review period:	Five years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Heritage and Information Governance

POLICY

HERIOT-WATT UNIVERSITY
DATA PROTECTION POLICY
CONTENTS

POLICY

1. INTRODUCTION

Heriot Watt University is an international community of learning and personal interaction is at the heart of our mission to create and to create and exchange knowledge for the benefit of society. The University's need to communicate and share personal data worldwide also presents significant data protection risks.

The University needs to collect, use and share personal information about students, staff and other individuals in order to deliver services, exercise its responsibilities and duties of care as an employer and provider of education and fulfil its legal and contractual obligations. In doing so the University must comply with the UK Data Protection Act, 1998, and equivalent legislation, such as the Malaysia Personal Data Protection Act, 2010, in other jurisdictions in which the University operates.

These laws require the University to protect personal information and control how it is used in accordance with the legal rights of the data subjects - the individuals whose personal data is held.

All staff, students and other data subjects are entitled to know

- What information the University holds and processes about them and why
- How to gain access to it
- How to keep it up to date
- What the University is doing to comply with its legal obligations under privacy law

2. PURPOSE

This policy and its supporting procedures and guidance aim to ensure that the University complies with its obligations as a Data Controller under the UK Data Protection Act, 1998 and processes all personal data in compliance with the Data Protection Principles which are set out in the Act.

In summary, these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subjects' rights.

POLICY

- Be kept safe from unauthorised access, accidental or deliberate loss or destruction.

- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Misuse of personal data, whether accidental or deliberate loss or disclosure to third parties, presents significant legal, financial and reputational risks including fines of up to £500,000 for serious breaches and loss of recruitment and research income.

In order to manage these risks, this policy sets out responsibilities for all managers, staff and contractors and anyone else that can access or use personal data in their work for the University.

The policy also sets out a framework of governance and accountability for data protection compliance across the University. It forms part 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

3. OBJECTIVES

The University will apply the Data Protection Principles to the management of all personal data throughout the information life cycle by adopting the following policy objectives.

We will:

3.1 **Apply "privacy by design" principles** when developing and managing information systems containing personal data.

This means that we will

- Use proportionate privacy impact assessment to identify and mitigate data protection risks at an early stage of project and process design for all new or updated systems and processes that present privacy concerns and in managing upgrades or enhancements to systems used to process personal data

- Adopt data minimisation: we will collect, disclose and retain the minimum personal data for the minimum time *necessary* for the

POLICY

purpose

- Anonymise personal data wherever necessary and appropriate, for instance when using it for statistical purposes

3.2 Process personal data fairly and lawfully

This means that we will

- Only collect and use personal data in accordance with the **conditions** set down under the Data Protection Act
- Ensure that if we collect someone's personal data for one purpose e.g. to provide advice on study skills, we will not reuse their data for a different purpose that the individual did not agree to or expect e.g. to promote goods and services for an external supplier
- Treat people fairly by using their personal data for purposes and in a way that they would reasonably expect

3.3 Seek informed consent when it is appropriate to do so

This means that we will seek the consent of individuals to collect and use their personal data

- Whenever the law requires us to do so, or
- Where their consent will be **specific, informed and freely given**.

In some circumstances, it is not appropriate to seek an individual's consent to process their data. For instance

- Where we are required to process personal data by law, for instance to comply with Home Office immigration rules, or
- Where we disclose personal data to the police to assist a criminal investigation and seeking the individual's consent would frustrate the purpose of the investigation by tipping off a suspect
- Where we need to process someone's personal data to fulfil a contract or our legitimate purposes, such as conducting examinations and assessments, and the individual cannot reasonably refuse or withdraw consent

We will explain

- What personal data collection is voluntary and why and the consequences of not providing it
- What personal data collection is mandatory and why we are entitled or obliged to process their data, for instance as a condition of employment or enrolment on a programme of study

POLICY

3.4 Inform data subjects what we are doing with their personal data

This means that, at the point that we collect personal data, we will explain in a clear and accessible way,

- What personal data we collect
- For what purposes
- Why we need it
- How we use it
- How we will protect their personal data
- To whom we may disclose it and why
- Where relevant, what personal data we publish and why
- How data subjects can update their personal data that we hold
- How long we intend to retain it

We will publish this information, tailored for students, staff and other groups of people on our website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them. We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them such as home addresses. Where we process personal data to keep people informed about University activities and events we will provide in each communication a simple way of opting out of further marketing communications.

In this way we will provide accountability for our use of personal data and demonstrate that we will manage people's data in accordance with their rights and expectations.

3.5 Uphold individual's rights as data subjects

This means that we will uphold their rights to

- Access a copy of the information comprising their personal data, responding to requests for their own personal data (subject access requests) in a fair, friendly and timely manner
- Object to processing that is likely to cause or is causing unwarranted and substantial damage or distress
- Prevent processing for direct marketing
- Object to decisions being taken by automated means
- Have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances
- Claim compensation for damages caused by a breach of the UK Data Protection Act

POLICY

3.6 Protect personal data

This means that we will

- Control access to personal data so that staff, contractors and other people working on University business can only see such personal data as is necessary for them to fulfil their duties

- Require all University staff, contractors, students and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles

- Set and monitor compliance with security standards for the management of personal data as part of the University's wider framework of information security policies and procedures

- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely and when working away from the University when their duties require this, for instance through provision of secure virtual private network, encryption and cloud solutions

- Take all reasonable steps to ensure that all suppliers, contractors, agents and other external bodies and individuals who process personal data for the University enter into our Data Processor Agreements and comply with auditable security controls to protect the data, in compliance with our **Procedures for approving, monitoring and reviewing personal data processing agreements** http://www.hw.ac.uk/staff/policies-governance/procedures/information-records.htm

- Maintain Data Sharing Agreements with educational partners and other external bodies with whom we may need to share student, staff personal data to deliver shared services or joint projects to ensure proper governance, accountability and control over the use of such data

- Ensure that our students are aware of how privacy law applies to their use of personal data in the course of their studies and how they can take appropriate steps to protect their own personal data and respect the privacy of others

- Manage all subject access and third party requests for personal information about staff, students and other data subjects in accordance with our **Procedures for responding to requests for personal data** http://www.hw.ac.uk/staff/policies-governance/procedures/information-records.htm

- Make appropriate and timeous arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for University business

POLICY

3.7 Retain personal data only as long as required

This means that we will

- Apply the University records retention policies relevant to each academic or professional service function
- Keep records locally only as long as required in accordance with these policies and then
- Destroy them securely in a manner appropriate to their format, or
- Transfer them by arrangement with Heritage and Information Governance for longer term storage or archival preservation

Some University records containing personal data are designated for permanent retention as archives for historical and statistical purposes. When managing access to archives containing personal data we will

- Apply exemptions to public rights of access to information as appropriate in accordance with the data subjects' rights to privacy
- Redact personal data, or
- Withhold specific categories of record, such as student records, for the lifetime of the student and their identifiable next of kin.

4. SCOPE

4.1 What information is included in the Policy

This policy applies to all personal data created or received in the course of University business in all formats, of any age. Personal data may be 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

Data subjects

These include, but are not confined to: prospective applicants, applicants to programmes and posts, current and former students, alumni, current and former employees, family members where emergency or next of kin contacts are held, workers employed through temping agencies, the members of the Court and members of the Committees of the Court, research subjects, external researchers, visiting scholars and volunteers, potential and actual donors, customers, conference delegates, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

POLICY

Users of personal data

The policy applies to anyone who obtains, records, can access, store or use personal data in the course of their work for the University. Users of personal data include employees and students of the University, contractors, suppliers, agents, University partners and external researchers and visitors.

4.3 Where the Policy applies

This policy applies to all locations from which University personal data is accessed 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 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 so that appropriate action can be taken to minimise harm.
- Informing the University of any changes to the information that they have provided to the University in connection with their employment or studies, for instance, changes of address

5.1 **The Principal and Vice–Chancellor,** as the Chief Executive Officer of the University, has ultimate accountability for the University's compliance with data protection law.

5.2 **The Secretary of the University** has senior management accountability for information governance including data protection management, 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 information governance including data protection 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 Head of Heritage and Information Governance** is the designated Data Protection Officer, who is responsible for recommending information governance and security strategy and ISMS to the Director of Governance

POLICY

and Legal Services and has executive oversight of policies, procedures and controls to manage information security and data protection.

5.5 **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 data protection management
- Managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data 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 data protection
- 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 Director of Information Services** is responsible for ensuring that centrally managed IT systems and services take account of relevant data protection risks and are integrated into the information security management system and for promoting good practice in IT security among relevant staff.

5.7 **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 data protection through the recruitment, induction, training, promotion, discipline and leaver management processes.

5.8 **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.

5.9 **The Head of Risk and Audit Management** is responsible for ensuring that data protection and wider 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.

5.10 **The Security and Operations Manager** is responsible for ensuring that controls to manage the physical security of the University take account of relevant data protection risks and are integrated into the information security management system.

5.11 **The University Information Governance and Security Group** is responsible for reviewing the effectiveness of data protection policies and procedures as part of its wider oversight of information security management, as set out in the Information Security Policy Framework.

POLICY

6. MONITORING AND EVALUATION

The Head of Heritage and Information Governance will monitor new and on-going data protection risks and update the information security risk register, reporting this promptly as required to the Director of Governance and Legal Services and the Head of Risk and Audit Management. 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 IT security risks related to data protection are captured on the register and that Schools, Institutes and Professional Service record data protection and information security risks on their local registers and escalate these as necessary to the Head of Risk and Audit Management.

6.1 The Chair and Clerk of the Information Governance and Security Group will make an annual report to the Risk and Project Management Strategy Group on compliance with the ISMS. 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 Secretary's Board and the Strategic Information Systems Committee as part of a wider communications strategy to promote a culture of responsible information security management across the University.

The Director of Governance and Legal Services is also responsible for meeting any reporting requirements of 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 University information security management systems.

These include

- Heads of Schools, Institutes and 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 management, and risk management and business continuity to deliver effective and proportional information security controls
- Review and refresh of all relevant policies and procedures

POLICY

- 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 forms part of an interconnected set of University Information Security Policies and procedures. These aim to develop a positive culture of information security throughout the University through the development of a holistic Information Security Management System (ISMS) to protect University information by maintaining its confidentiality, integrity and availability.

This policy should be read in conjunction with 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 policies are published on the University website at http://www.hw.ac.uk/staff/policies-governance/procedures/information-records.htm

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

8.2 Legal Requirements and external standards

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

- Computer Misuse Act 1990
- Data Protection Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002
- Privacy and Electronic Communications Regulations 2003

POLICY

- 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/

Laws of Malaysia: Act 709: Personal Data Protection Act 2010
http://kpkk.gov.my/images/dmdocuments/Personal_Data_Protection_Act_2010.pdf

UK Information Commissioner's Office (ICO)
Statutory Codes of Practice, including:

- Anonymisation
- CCTV
- Data Sharing
- Employment Practices
- Personal Information Online
- Privacy Notices
- Subject Access

Guidance, including:

- Bring Your Own Device
- Cloud Computing
- Data controllers and data processors: what the difference is and what the governance implications are
- Data security breach management
- International Data Transfers
- IT Asset Disposal
- Privacy and Electronic Communications
- Privacy Impact Assessment

http://www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications

JISC Legal: Data Protection Code of Practice for FE and HE, 2008
http://www.jisclegal.ac.uk/Portals/12/Repository/Data%20Protection%20Code%20of%20Practice%20for%20FE%20and%20HE.pdf

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.

POLICY

Personal Data	Information in any format that relates to a living person who can be identified from that information or other information held by the University, its contractors, agents and partners or other third parties. Although the Data Protection Act applies 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.
Sensitive Personal Data	Sensitive personal data (as defined in Section 2 of the Data Protection Act 1998) is personal data relating to an identifiable individual's a) racial or ethnic origin; b) political opinions; c) religious or other beliefs; d) membership of a trade union; e) physical or mental health or condition; f) sexual life; g) proven or alleged offences, including any legal proceedings and their outcome In addition, the University definition of High Risk Confidential Information includes the following personal data: Any other information that would cause significant damage or distress to an individual it was disclosed without their consent, such as bank account and financial information, marks or grades
Data Controller	An organisation which determines the purposes for which personal data is processed and is legally accountable for the personal data that it collects and uses or contracts with others to process on its behalf
Data Processor	In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	A person whose personal data is held by the University or any other organisation
Processing	Creating, storing, accessing, using, sharing, disclosing, altering, updating, destroying or deleting personal data

POLICY

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 (ISMS)

"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, policies, 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 information security contact:
Heritage and Information Governance
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 16/04/2014	Supersedes policy approved 2002 and personal data processor policy approved 2009	Court; on the recommendation of the Audit and Risk Committee, University Executive and Secretary's Board	Updated to take account of legal developments and University internationalisation and risk environment; Supporting Procedures for Data Processor agreement to incorporate content of Data Processor Policy.

POLICY

Appendix 1

Conditions for processing personal data
The individual who the personal data is about has consented to the processing.
The processing is necessary: - in relation to a contract which the individual has entered into; or - because the individual has asked for something to be done so they can enter into a contract.
The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
The processing is necessary for • the legitimate interests of the data controller, or • the third party or parties to whom the data are disclosed, **Except** where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject

POLICY

Appendix 2

Conditions for processing sensitive personal data
The individual who the sensitive personal data is about has given explicit consent to the processing.
The processing is necessary so that the University can comply with employment law.
The processing is necessary to protect the vital interests of: - • the individual (in a case where the individual's consent cannot be given or reasonably obtained), • another person (in a case where the individual's consent has been unreasonably withheld).
The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
The individual has deliberately made the information public.
The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
The processing is necessary for administering justice, or for exercising statutory or governmental functions.
The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.
The processing is in the substantial public interest, and is necessary for • prevention or detection of any unlawful act; and • must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.
The processing is in the substantial public interest, and is necessary for • the discharge of any function which is designed for protecting members of the public against (i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or . (ii) mismanagement in the administration of, or failures in services provided by, anybody or association; and • must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function.
The disclosure of personal data is in the substantial public interest in connection with (i) the commission by any person of any unlawful act (whether alleged or established),

POLICY

(ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or
(iii) mismanagement in the administration of, or failures in services provided by, anybody or association (whether alleged or established);

- is for journalism, artistic or literary purposes, and
- is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.

The processing is in the substantial public interest and is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and carried out without the explicit consent of the data subject because the processing

(i) is necessary in a case where consent cannot be given by the data subject,
(ii)is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or
(iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

The processing is necessary for the purpose of
(i) carrying on insurance business, or
(ii) making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme

- is of sensitive personal data consisting of information falling within section 2(e) of the Act relating to a data subject who is the parent, grandparent, great grandparent or sibling of the insured person, or (ii)in the case of paragraph (a)(ii), the member of the scheme;
- is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of that data subject and the data controller is not aware of the data subject withholding his consent; and
- does not support measures or decisions with respect to that data subject.

The processing is in the substantial public interest and is

- necessary for research purposes
- does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
- does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

POLICY