Information Security
Policy for secure use of confidential information on portable media

1. Introduction

This policy is a constituent part of the **University Information Security Policy** which sets out a framework of governance and accountability for information security management across the University.

Heriot-Watt University relies on the effective management and flow of information to enable staff to communicate and work effectively worldwide on University business.

The University recognises that the loss or theft of personal data and other confidential information can have devastating consequences for individuals and severe financial, legal and reputational costs to the organisation, including significant fines from the UK Information Commissioner.

2. Policy Statement

This policy has been developed to enable staff, students and other authorised users to use, share and communicate confidential information appropriately and securely, when it is necessary for them to do so on University business. This policy reflects good practice that is currently being adhered to in other Higher Education Institutions and the requirements placed upon the University by its auditors, insurers and external funders, contractors and partners.

This policy and the procedures that support it have been developed to reduce the risks of the loss of **HIGH RISK** and **MEDIUM RISK** confidential data held on portable media. The University recognises that in the vast majority of cases, losses of confidential information are caused by human error- a USB stick or paper file is lost or mislaid, or in circumstances beyond the individual's immediate control e.g. a laptop is stolen from someone's flat or their car.

To reduce this risk, all staff, students and other users given access to University information must take the simple common sense precaution of not downloading confidential data to portable media or taking it out of paper filing systems and away from the workplace unless this is absolutely necessary to conduct University business.

Some categories of confidential information are more sensitive than others

POLICY

HIGH RISK confidential information is defined as:

- Any privileged or proprietary information that could cause significant harm (including operational financial, legal or reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

- High risk personal data is information that would cause significant damage or distress to an individual if it was disclosed without their consent.

MEDIUM RISK confidential information is defined as:

- Information that must not be disclosed to any member of staff, student or other person who does not have a legitimate need to access the information in the course of their work for the University

Further information and examples of HIGH, MEDIUM and LOW RISK information can be found in Appendix A.

Data "Owners" of University databases, e.g. Oracle Financials, Human Resources, Payroll, SAS/ISS or contacts, alumni and fundraising will identify **HIGH RISK** confidential data e.g. salaries of identifiable staff held within those databases and staff who are authorised to access this data. The data owner must approve in advance the download of data from these systems.

Data "Owners", Heads of Schools, Institutes and Professional Services will identify other **HIGH RISK** confidential information in their areas of responsibility and staff who are authorised to access this information. The data owner must approve in advance the use of this confidential information away from the workplace. An example of HIGH RISK data is information received under a confidentiality agreement from a research funder, contractor or supplier. The Information Security Officer will provide further guidance and advise managers and staff on practical measures to protect confidential information in each business unit.

All **HIGH RISK** confidential data downloaded from University databases and other information systems or sent by email must be encrypted in accordance with the minimum standard: 256 bit Advanced Encryption System (AES).

All **MEDIUM RISK** confidential data downloaded to portable devices or sent as attachments to emails must be protected with a strong password.

All laptops and other portable devices purchased for University business must be issued with strong passwords.

All staff, students and other users given permission by Data "Owners", Heads of Schools, Institutes and Professional Services to use **HIGH RISK** and **MEDIUM RISK** confidential information, in any format, away from the workplace will take appropriate measures to maintain the security of this information at all times. These measures are set out in Appendix B: **Conditions for use of confidential information away from the workplace**

POLICY

Information held on a portable device must always be a *copy* of an original held on a University computer system. This is necessary to ensure that this information remains accessible to authorised users even if the portable device is lost, damaged or stolen.

If you suspect that confidential information in your care has been lost, stolen, tampered with or disclosed without authorisation, report the incident immediately to the **Information Security Officer** on 0131 451 3274/3219 or email foi@hw.ac.uk. Prompt reporting of problems will enable staff to take effective action to mitigate the consequences.

3. Key Principles

Many staff are required to use and communicate confidential information in the course of their work, by using University email systems. Examples include a lecturer and student discussing feedback on an assignment, members of a management committee discussing actions arising from a meeting or a reviewee sending a reviewer their draft performance and development review or forward job plan.

This policy is not intended to stifle the vital flow of confidential data necessary to keep the University working effectively. However, all users of confidential University information have a responsibility to take appropriate measures to minimise the risk of this data falling into the hands of people who do not have the right to see it.

The University takes its responsibilities for information security very seriously. Failure to comply with this policy is a disciplinary offence which may include action up to and including dismissal. Serious breaches of the policy, whether intentional or non-intentional, and which place the University at serious financial, commercial or reputational risk or actual loss may be considered as gross misconduct offences, for which summary dismissal may be an outcome.

4. Scope

This policy applies to
All staff and students working for or on behalf of the University and other users given access to University information

All HIGH RISK and MEDIUM RISK confidential information created or received by the University in all formats that is

- stored on portable devices and media,
- transported from the workplace physically or electronically
- accessed remotely.

5 Responsibilities

All staff, students and other users given access to University information are responsible for adhering to this policy.

Heads and managers and staff of Schools, Institutes and Professional Services are responsible for identifying specific categories of **HIGH RISK** and **MEDIUM RISK** confidential information in their areas, authorising and monitoring access to this information and agreeing appropriate measures with the Information Security Officer to prevent unauthorised access.

POLICY

Heads of Schools and Services will buy encrypted USB memory sticks which meet the minimum security standard: 256 bit Advanced Encryption System (AES) from Procurement Services or another designated University stockholder and issue them to authorised users, keeping a record of USB sticks and passwords issued so that they can be traced and the information retrieved if the USB stick is lost or the user forgets the password.

Staff who are authorised to use their own pre-encrypted USB sticks or encryption tools must adhere to the minimum standard: 256 bit Advanced Encryption System (AES).

The University Archivist, as Information Security Officer, is responsible for recommending policies and procedures to meet the University's information security requirements, offering advice and support to staff and monitoring compliance with information Security Policy and procedures.

6. Link with other policies
This policy and procedure forms part of the University Information Security Policy 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.

7. Review date
The University Information Security Group will review this policy in April 2011 and recommend any changes to the Risk Management Strategy Group, the Infrastructure Board and the Planning and Management Executive.

8. For further information and advice
about this policy and any aspect of information security contact:
Information Security Officer:
Telephone: 0131 451 3274/3219
Email: foi@hw.ac.uk

POLICY

Appendices

These appendices contain supporting guidance and procedures which will be revised and updated by the Information Security Group as needed in line with operational requirements and good practice.

Appendix A

Definitions

1. Portable device means any:

- Laptop computer
- Personal Digital Assistant (PDA) or palmtop
- Phone, Smartphone, MP3 player or other communications / audio / video device with data storage capability

2. Portable medium means any:

- CD, DVD, floppy disk, tape, zip disk, etc
- external hard disk
- USB memory stick
- Solid-state or other storage card (e.g. CompactFlash, SD, other new digital storage, etc)
- Records and documents in hard copy format

3. Information Security Classification Scheme

Confidential information

This is a broad category of information that technically includes any information in any format (electronic or paper) created or received by a member of staff in the course of University business that would be exempt from the public right of access under the Freedom of Information (Scotland) Act 2002 (FOISA). This includes any personal data that has not already been disclosed with the consent of the person who is the subject of that data. Personal data is information about a living person who can be identified by that information, ether by itself or in combination with other data.

HIGH RISK confidential information (RED) is

- Any privileged or proprietary information that could cause significant harm (including operational financial, legal or reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

- High risk personal data is information that would cause significant damage or distress to an individual if it was disclosed without their consent.

It is recognised that **HIGH RISK** confidential information cannot be comprehensively defined for the purposes of a policy without being unduly prescriptive. The definition

of **HIGH RISK** can depend on context. The unauthorised disclosure of one person's home address may cause annoyance in one case or real harm in another where that person's personal circumstances put them at risk.

In order to make this policy as relevant and helpful as possible the Information Security Officer will provide guidance and advice to data "owners" and users, Heads and managers and staff of Schools, Institutes and Professional Services to help them identify specific categories of **HIGH RISK** confidential information in their areas.

As the University holds a significant amount of personal data about students we will also consider the views of students through consultation with representatives of the Heriot-Watt University Students Association.

Examples of confidential information that are considered **HIGH RISK** and **must** be protected from loss, misuse and unauthorised disclosure are

HIGH RISK personal data

- Sensitive personal information (as defined in Section 2 of the Data Protection Act 1998 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 e.g. a court sentence imposed on the individual

- Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas;

- Personal information relating to vulnerable adults and children;

- Detailed profiles of individuals; including information about work performance, salaries or personal life *that would cause significant damage or distress to that person if disclosed*;

- Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or

- Sensitive negotiations which could adversely affect individuals.

- Security information that would compromise the safety of individuals if disclosed.

POLICY

Other categories of "high risk" information

- Unpublished research data **that has been received or created under conditions of confidentiality** and would if lost or disclosed significantly impact on the success of a research project, research income. REF outputs or knowledge transfer

- Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners

- Information that would substantially prejudice the University or another party's commercial interests or competitive edge if it were disclosed e.g. detailed financial and strategic plans

- Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced.

- Information that would compromise the security of buildings, equipment or assets if disclosed.

MEDIUM RISK: (AMBER)

Information that must not be disclosed to any member of staff, student or other person who does not have a legitimate need to access the information in the course of their work for the University

Information (other than personal data) that must not be disclosed without the permission of the data owner.
Personal data that must not be disclosed to third parties unless

- The consent of the person who is the subject of the data has been obtained or
- another Condition for processing the data set out in the Data Protection Act 1998 has been met.

Examples of information that can be shared by email between individuals with a legitimate "need to know" but not disseminated more widely

- Information and feedback about individual progress between a lecturer and a student

- Committee papers on matters of current business that are not intended for wider dissemination or consultation, and draft minutes issued by committee members; discussions of actions arising with others who need to take them forward

- Draft Performance and Development Review or Forward Job Plan between the reviewee, reviewer and countersigatory and the person responsible for filing confidential information for the School/Institute or Service

LOW RISK (GREEN)

- Information that has been produced and signed off by the data owner for publication or for public access

Information that is designated as accessible on demand within the University's **Publication Scheme**.

- A published research paper

- A guidance document for students signed off for distribution by the relevant service head

- The minutes of a committee of Court or Senate, once the minutes have been approved by the Convener and redacted to remove any information that is exempt from disclosure under the Freedom of Information (Scotland) Act 2002 (FOISA).

POLICY

Appendix B

Conditions for use of HIGH RISK and MEDIUM RISK confidential information away from the workplace

The following conditions apply specifically to use of HIGH RISK confidential information

If it is essential to University business that staff, students or other users have access to **HIGH RISK** confidential information away from the workplace:

Heads of Schools, Institutes and Professional Services, or their designates are responsible for

- authorising such use
- keeping a record of individual staff who are permitted to access and use high risk confidential information in this way
- keeping a register of encrypted USB memory sticks and passwords issued to individual users.

Staff, students and other users of University information are responsible for Obtaining written authorisation from your line manager or the data owner e.g. by exchange of emails.

Obtaining a pre-encrypted USB stick from the data security contact for your School, Institute or Service, and informing them if you change the password

Ensuring that if you are authorised to use your own pre-encrypted USB sticks or encryption tools these must adhere to the minimum standard: 256 bit Advanced Encryption System (AES).

The following conditions apply to use of HIGH RISK and MEDIUM RISK confidential information

You may download confidential information onto portable devices, use it to work away from your workplace and communicate it to people and organisations that are authorised to receive it **if you first ensure that the following conditions have been met:**

You take appropriate measures to maintain the security of this information at all times

- HIGH RISK confidential information stored or communicated in electronic format must be encrypted.

- MEDIUM RISK confidential data downloaded to portable devices or sent as attachments to emails must be protected with a strong password, which is at least 8 characters long and combines letters and numbers.

- Information held on a portable device must always be a *copy* of an original held on a University computer system. Portable devices must not be used as the only repository of a university document- because if the device is lost that document is also lost to you and the University

- Information in hard copy format must be transported securely under your supervision at all times or by guaranteed secure courier service and locked away when not in use. Confidential information in any format must not be left unsupervised in a vehicle, even in the boot.

- Remote access to University information systems must be through a Virtual Private Network (VPN) or equivalent secure mechanism. Unencrypted confidential data must not be downloaded onto home PCs.

POLICY