University of Reading

Policy on processing personal data and sensitive information off campus or on an external network ('the Encryption Policy')

1 Purpose and scope

This document sets out the University's policy on processing personal data and sensitive information off campus or on an external network, including the use of portable and mobile equipment.

Its aim is to ensure that the University complies with data protection legislation and that sensitive information is protected from unauthorised access, dissemination, alteration or deletion. It complements and supports the existing **Data Protection Policy** and **Guidelines**.

It applies to all University staff students and others who process sensitive information off campus or on external networks on behalf of the University. It covers the use of mobile devices (e.g. laptops, tablets, smartphones), portable storage media (e.g. memory sticks or CDs), remote computers, or other forms of communication (e.g. email and instant messaging).

2 Definitions

Processing – means any operation on data, including organisation, adaptation and alteration; retrieval, consultation or use; disclosure, transmission, dissemination and otherwise making available; or alignment, combination, blocking, erasure and destruction. Processing includes the sending of information via email and other mechanisms such as Instant Messaging and Twitter.

Sensitive information – includes, for example, confidential information, information critical to the business continuity of the University, research data subject to contractual non-disclosure agreements and information held in business critical applications. Further examples are given below.

Personal data – the legal and technical definition of 'personal data' is complex, however staff should treat information about living, identifiable individuals as 'personal data'. Specific examples are given in 7 below.

External network – is either provided by a third party (for example an ISP or mobile provider) or is part of the University's guest network provision (including eduroam). This covers any use of mobile devices when processing University information.

Encryption – the process of converting information so that it cannot be read by unauthorised people.

3 Consequences of non-compliance

Failure to comply with this policy may expose the University, its staff or students to risks including fraud, identity theft and distress, or damage the University's reputation and its relationship with its stakeholders, including research funders. Regulators can impose monetary penalties of up to £500,000 on the University for breaches of data protection legislation.

4 Background

The Data Protection Act 1998 sets out how the University may use personal data. Principle seven of the Act states:

> *'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'*

Compliance with the above Principle involves a judgment as to what measures are appropriate in particular circumstances; this policy provides guidance on how to make this judgment when processing high risk personal data or sensitive information on an external network. Regulators in other juristictions also have requirements for keeping data secure.

5 Policy statement

If high risk personal data or sensitive information is to be processed off campus or on an external network, then it must be stored and transmitted in an encrypted form of the required standard[1].

[1] Any exceptions to this policy statement must be authorised by the Director of IT.

6 Key principles

The following key principles underpin the policy statement in 5 above and this policy generally. All staff must comply with these principles when using mobile devices and portable storage media or otherwise processing personal data or sensitive information on an external network.

a. Avoid processing personal data whenever possible.

b. If processing personal data is necessary, then consider anonymising the information to obscure the identity of the individuals concerned. Further guidance on anonymisation can be found at **http://www.data-archive.ac.uk/create-manage/consent-ethics/anonymisation**.

c. Use the University's central and secure shared drives to store and access personal data and sensitive information; this helps to ensure that only legitimate users have access to it.

d. Use the IT-authorised remote access facilities that are both secure and encrypted to access personal data and sensitive information on the central servers instead of transporting it on mobile devices and portable media.

e. Do not use non IT-authorised third party hosting services, like Dropbox or Google Mail, when processing high risk personal data or sensitive information.

f. If there is no option but to use mobile devices, portable media or email for high risk personal data or sensitive information, use encrypted devices or encryption software.

g. Do not use personal equipment, such as home PCs or personal USB sticks, to process high risk personal data or sensitive information.

h. Avoid sending high risk personal data or sensitive information by email or using email to store such information. If you must use email to send this sort of information, encrypt it [www.reading.ac.uk/encryption-files-guidance]. If you are sending unencrypted high risk personal data or sensitive information to another University email account, indicate in the email subject line that the email contains sensitive information so that the recipient can exercise caution about where and when they open it.

i. Do not process high risk personal data or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk personal data or sensitive information to an insecure device.

j. Consider the physical security of high risk personal data or sensitive information, for example use locked filing cabinets/cupboards for storage.

k. Implement the University's **records management policy** and **retention and disposal policies** so that you do not keep personal data and sensitive information that you do not need. If there are no suitable retention and disposal policies in place for your area, contact your **IMPS Contact** to arrange to put some in place.

l. Where the master copy of record is held in an electronic form, it should be stored on university servers. In identifying master copies of record, staff should seek advice from their IMPS contact.

m. Electronic keys for encryption, eg passwords, must be appropriately managed so that the University can always access the information.

n. When sending encrypted data outside the UK, have regard for the regulatory regime in the destination country.

o. Ensure that any third party working with any University-owned information as set out under 7 below handles it in accordance with the policy statement under 5. This includes ensuring that, where such data is returned from that third party to the University, it is transmitted in encrypted form.

p. Encryption keys, eg passwords, must not be communicated via the same channel as the encrypted data. Follow www.reading.ac.uk/encryption-files-guidance for further information.

7 High risk personal data or sensitive information

The following are examples of high risk personal data or sensitive information:

a. Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to, students, staff, alumni, research participants.

b. Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary

c. Information relating to 10 or more members of staffs' performance, grading, promotion or personal and family lives.

d. Information relating to 10 or more alumni/students' programmes of study, grades, progression, or personal and family lives.

e. Any set of data relating to 5 or more living, identifiable individuals' health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.

f. Information relating to identifiable research participants, other than information in the public domain.

g. Information that would be likely to disadvantage the University in funding, commercial or policy negotiations.

h. Information provided to the University in confidence.

i. Finance data held in Agresso and any payment card data covered by PCIDSS security requirements.

j. Health records of any living, identifiable individual.

k. Discussion papers and options relating to proposed changes to high profile University strategies, policies and procedures, such as the University's undergraduate admissions policy, before the changes are announced.

l. Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.

m. Information that would attract legal professional privilege.

8 Required encryption standards

The required standard of encryption is AES 256 bit, FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197. Encryption products certified via CESG's CPA or CAPS schemes to at least FOUNDATION grade would also meet the required standard.

9 Guidance and support

Further support is available from:

- IMPS, imps@reading.ac.uk on records management and data protection
- IT, its-help@reading.ac.uk on the technical aspects of security

Further specific guidance is available here:

- How to encrypt
  - **Introduction to encryption**
  - **Files** including email attachments
  - **Storage**
  - **Memory/USB sticks**
- **Mobile devices**
- **Information handling**
- **Remote working**
- **Online Information Security training module**

10 Acknowledgements

This policy and supporting guidance is based on the University of Edinburgh's approach to encryption which can be found here:

http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/guidance-policies/encrypting-sensitive-data

Latest version	Keeper	Reviewed	Approved by	Approval date
Version 1.0	IMPS	Annually	IFSG	04/09/12
Version 1.1	IMPS	Annually	Information Security WG	08/11/13
Version 1.2	IMPS	Annually	ISWG	23/01/15