UNIVERSITY OF LEEDS

Information Protection Policy

Version 1.2

March 2016

Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes
1.0	10/03/13	www.leeds.ac.uk/informationsecurity	First formal issue
1.1	21/06/13	www.leeds.ac.uk/informationsecurity	1. Added 'unrestricted' to para 5. 2. Addition to Cloud para 6. 3. Advice on mobile protection in 12. 4. Safe haven fax added to table.
1.2	10/03/16	www.leeds.ac.uk/informationsecurity	Updated broken links

Version Awareness

The audience of this document should be aware that a printed copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://www.leeds.ac.uk/informationsecurity. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

Introduction

This policy sets out the steps which members of the University are required to take to protect the security of all 'sensitive information', a category which includes but is not confined to information that relates to and identifies individuals ('personal data'). The policy applies in particular to members of staff, but it also covers students wherever appropriate.

Overview

The Policy classifies sensitive information according to its damage potential, and defines the special controls which are to be applied in order to protect it from inappropriate disclosure. There are two kinds of classified information: 'confidential' and 'highly confidential'.

Any information that is not categorised as either 'confidential' or 'highly confidential' is 'unclassified'. No particular controls apply to the disclosure of unclassified material.

- **Highly confidential** applies to information disclosure of which to unauthorised recipients would be likely to result in *serious damage* to the interests of individuals or of the University.
- **Confidential** applies to information disclosure of which to unauthorised recipients could have a *negative impact* on individuals or the University.

Except for information which is obviously and legitimately in the public domain (such as job titles and departments), personal data will, as a general rule, fall into one or other of the classified categories.

The scale, volume and the medium of storage need to be taken into account in the assessment of the classification of any set of information. For example, information which in itself would be classified as 'confidential' when it relates to just one individual might need to be classified as 'highly confidential' when it covers hundreds or thousands of individuals, especially (but not only) if it is held in electronic form. The potential for damage from unauthorised disclosure is very much higher in the latter case than in the former and the level of control needs accordingly to be higher.

Examples of material falling into the above categories are set out in Annex 1.

Requirements

The University is seeking to create and reinforce a culture which takes data security seriously. To this end, all members of the University are expected to comply with the following requirements.

1. Assess the sensitivity of all information you create and receive; and take proportionate measures to ensure that data are held securely. Guidance on whether or not documents should be classified (as 'confidential' or 'highly confidential'), and the key controls for protecting data, are set out in the annexes to this policy. (Further guidance is available at http://it.leeds.ac.uk/downloads/download/43/example_risk_assessment_form

2. Keep personal passwords secret; never share them. Group passwords must not be disclosed outside the group. (Guidance on passwords is available at http://it.leeds.ac.uk/info/117/guides_and_other_documents/772/selecting_a_strong_password)

3. Access or share classified information only where the conduct of University business requires you to do so and with the necessary permissions.

4. Obtain any necessary permissions before sharing classified information with colleagues or third parties. Seek advice if you are unsure what you need to do (see contact information below).

5. Keep electronic data on the University's servers. In general, store classified data only on the University's servers (first encrypting any highly confidential data that is to be kept in unrestricted shared areas). (See also 14 below.)

6. Unless using a bespoke service that has been security-tested and approved by the University, Cloud services[1] must not be used for storing or processing data which is (a) classified; (b) of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted; or (c) valuable intellectual property of the University (on which further advice can be sought from the Legal Adviser).

7. Make sure no one can access your computer when it is left logged on and unattended. Use 'password protection' on your computer and on any portable electronic equipment used to store or access University data (including mobile phones used to access e-mail).

8. Comply with the University's Code of Practice on Data Protection (see http://www.leeds.ac.uk/secretariat/data_protection_code_of_practice.html) In particular, anonymise research data wherever possible, only take the data you need; and in any event do not keep data longer than required for the conduct of University business.

9. Never configure your computer (or other hardware) *automatically* to forward University e-mails to an external service provider (for example, a personal hotmail account).

10. When e-mailing classified information to other members of the University, always use their University e-mail address (rather than externally-hosted e-mail facilities.)

11. When e-mailing data, always double-check that you have used the right address before sending the e-mail. This is particularly necessary when your e-mail system 'predicts' the intended recipient from your first few key strokes.

12. When you are off campus, use University-approved methods to access University e-mail or data (such as Outlook Web Access or Citrix for example). If you use mobile devices for this purpose, make sure they are password or pin protected, or otherwise encrypted.

13. Encrypt classified electronic data (a) when holding them on laptops or memory sticks or other removable media[2] and (b) before attaching them to e-mails. Never include 'highly confidential' information within the body of an unencrypted e-mail.

14. If you have to keep classified data on laptops, memory sticks and other portable devices, do so **only** on a temporary basis. Delete such information from the portable device at the earliest possible opportunity. Keep the volume of data on a memory

[1] Examples of cloud services include iCloud, Dropbox, Microsoft (Azure, BPOS and SPLA), Amazon (AWS, S3 and EC2) and Google (Google Apps). Advice on approval of bespoke solutions should be sought from the IT Security Coordinator.
[2] This requires the use of the University Encryption Standard. Even those who do not routinely handle classified data may wish to encrypt their laptops. Details are available via the ISS Help Desk.

stick or similar device to the absolute minimum required for immediate operational purposes.

15. Save in very exceptional circumstances, and with the permission of your line manager, highly confidential paper documents should not be taken outside the University; if you have to take classified paper documents outside the University, do so for the shortest time possible, keeping them securely. If you obtain classified information outside the University (for example, through the collection of research data), keep the data securely, and bring or post them into the University at the earliest opportunity.

16. If posting classified material, use a first class envelope for confidential material, and use recorded post and a double envelope (one inside the other) for material that is highly confidential. The external envelope must not bear the classification.

17. Use shredding machines for disposal of classified paper documents. Disposal of bulk classified waste can be carried out through Cleaning Services. Any unwanted, damaged or obsolete computer hardware must be disposed of through Cleaning Services – it cannot be sold or donated to members of the University or to other organisations, such as charities. Seek advice if you are unsure what to do.

18. Ensure offices are locked when they are unattended, and that classified papers are locked away when not in use.

19. Make sure any third parties (including contractors) permitted to handle classified data are required to take appropriate security measures. (A template for use in this connection is available from the Legal Adviser.) Similarly, respect any additional third party rules relating to data that has been shared with the University – for example, by the NHS.

20. If you use a home or other non-University computer to create or access classified information, make sure that the computer has up-to-date security protection, and that no-one else can use it to view University information. Classified data must not be stored on privately-owned computers and equipment.

Overall responsibility for information security issues within the University rests with Roger Gair, the University Secretary. Assistance and training can be provided through Kevin Darley, the University's IT Security Co-ordinator (k.j.darley@leeds.ac.uk; ☎ 0113 343 1118) or from Adrian Slater, the University's Legal Adviser (a.j.slater@leeds.ac.uk).

Any information security incidents or breaches must be reported to one or other of them immediately.

ANNEX 1 – Classifying information

Personal Data		
Unclassified	**Confidential**	**Highly Confidential**
Anonymised data[3] Data agreed by data subjects to be put into the public domain. Publicly available staff directories including work telephone numbers, e-mail address and Department information. Simple list of names with no other data. Information on individuals available through social network sites where information provided on condition that will be public domain information. Final degree classification.	Individual's passport details, home address and telephone number. Individual's name plus home address/postcode, age and home telephone numbers. List of student names and their student ID number or list of staff names and their personnel number. Names and addresses of student applicants to the University. Attendance details relating to an existing student. Student transcript Exam scripts Exam marks Examiner's comments on a student's performance	Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees). Information on individual's racial or ethnic origin, political opinion, religious or other beliefs, physical or mental health or criminal record. Attendance and academic progression information/ disciplinary information relating to an existing University student. Preliminary degree classification/ transcript information pending formal approval and any publication
	References for students or staff[4]	
	UCAS forms[4]	
Dates of birth.	Individual's name plus date of birth or national insurance number.[5]	Individual's name plus date of birth or national insurance number, passport details, home address and telephone number[5]. Hundreds of individuals' names plus date of birth or national insurance number[3]

[3] For these purposes anonymised data is data which does not relate to a living individual and cannot identify an individual, or cannot identify an individual through other information which is in the possession of, or is likely to come into the possession of the organisation processing (see section 1 (1) (a) of the DPA 1998
[4] Content dependent e.g information relating to health, criminal record or disciplinary matters, would make the reference/UCAS form highly confidential.
[5] Adding additional combinations of data can change the overall status. Simply increasing the volume of data can also change status

Non-Personal Data		
Unclassified	**Confidential**	**Highly confidential**
	Research grant applications/proposals[6] Information relating to supply or procurement of goods/services prior to approved publication.	
Information contained within an organisation's annual corporate report. Information that can be obtained from publicly available directories or regulatory bodies e.g. Companies House or HEFCE. Information contained within an organisation's web sites for public dissemination.	Assessment material prior to "unseen" assessment	Future marketing or student fees information not yet agreed to be made public. Other information that may be regarded as a trade secret or otherwise highly commercially sensitive. Information relating to restricted intellectual property rights or otherwise covered by a confidentiality agreement/ contractual term. Legal advice and other information relating to legal action against or by the University.

Please be aware that the above are only indicative general examples of personal and non personal data. As highlighted in the footnotes and main body of the policy, the mix of information, the amount of information and the medium in which the information is held can change the classifications.

[6] Content dependent e.g. information subject to imminent academic publication or industrial collaborators may lead to application/proposal being highly confidential.

ANNEX 2: Key controls for protecting classified information

Activity	Confidential	Highly Confidential
➢ *Electronic data*		
Storage of data in *shared* areas of University server	Yes	Only if encrypted
Storage of data in personal area of University server	Yes	Yes
Remote access to the data	Yes, but only via Citrix or other University-approved mechanism	Yes, but only via Citrix or other University-approved mechanism[7]
Storage of data on University-owned laptops or other portable devices.	Only on a temporary basis and only if encrypted	Only on a temporary basis and only if encrypted
Storage of data on privately-owned laptops or other portable devices (including memory sticks)	No	No
Sending data by e-mail	Yes (taking care to check the address of the recipient(s))	Yes but only as encrypted attachment
➢ *Paper and other media*		
Storage in University	Locked filing cabinet or equivalent	Locked filing cabinet or equivalent inside room normally kept locked
Facsimile transmission	Yes	No (unless directed to a 'safe haven' machine)
Data collection outside the University	Kept securely on the person (and returned to the University at the earliest opportunity)	Kept securely on the person, preferably in a locked case (and returned to the University at the earliest opportunity)
Taking documents off campus	For the shortest time possible and documents to be kept securely about the person	Only permitted exceptionally and once authorised by your line manager
Posted	Yes via first class post in an envelope without any classification marking	Yes, via Recorded[8] post when double enveloped, without classification marking on outer
Disposal	Shred small volumes. Bulk disposal through cleaning services.	Shred small volumes. Bulk disposal through cleaning services.

[7] Remote access to unencrypted information is possible only to information in the personal area of a server.
[8] Recorded post requires a signature from the recipient; other forms of post requiring a signature (e.g. Special Delivery) are also legitimate.