

Policy on the Storage, Transmission and Use of Personal Data and Sensitive Business Information Outwith the University Computing Environment

Purpose

This document sets out the University's policy on the storage, transmission and use of personal data and sensitive business information out with the University computing environment, including on mobile devices and portable storage media.

Its aim is to ensure that the University complies with the Data Protection Act 1998 and that sensitive business information is protected from unauthorised access, dissemination, alteration or deletion.

Audience

This policy applies to all University staff who store, transmit and use personal data and sensitive business information out with the University computing environment, including using mobile devices (e.g. laptops, blackberries), portable storage media (e.g. memory sticks or CDs) or other forms of communication (e.g. email).

Scope

1. The definition of "personal data" is complex, but for day-to-day purposes it is advisable to treat all information about living, identifiable individuals as "personal data". The definitions section below gives examples of high and medium risk personal data and business information.
2. For the purposes of this policy, personal data and business information might be in a variety of formats, including but not limited to email, word processed documents, spreadsheets and databases.

Consequences of non-compliance

3. Failure to comply with this policy could 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.
4. The Information Commissioner can also levy a fine on the University, which may be up to 10% of the University's turnover. For example, in July 2009 three HSBC firms were fined £3.2 million for sending unencrypted personal data by courier and post.

Background

5. The Data Protection Act 1998 sets out how organisations may use personal data. It 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.”
6. This requirement involves a judgement as to what measures are appropriate in particular circumstances. This policy provides guidance for University staff on how to make this judgement when using, transporting or storing personal data or highly sensitive information out with the University computing environment.

Policy statement

7. Medium and high risk personal data or business information must be encrypted if it leaves the University environment.

Key principles

8. The following key principles underpin the University’s policy on the storage, transmission and use of personal data and sensitive business information out with the University computing environment. All staff must comply with these principles when using mobile devices and portable storage media or otherwise removing information out with the University computing environment.
 - a. Avoid using personal data wherever possible.
 - b. If the use of personal data is unavoidable, consider partially or fully anonymising the information to obscure the identity of the individuals concerned.
 - [Anonymisation FAQs](#)
 - <http://www.recordsmanagement.ed.ac.uk/InfoStaff/FAQs/Topic6.htm>
 - c. Use the University’s secure shared drives to store and access personal data and sensitive business information, ensuring that only those who need to use this information have access to it.
 - d. Use remote access facilities to access personal data and sensitive business information on the central server instead of transporting it on mobile devices and portable media or using third party hosting services.
 - e. If there is no option but to use mobile devices, portable media or email for high and medium risk personal data or business information, buy encrypted memory sticks or use encryption software.
 - f. Do not use personal equipment (such as home PCs or personal USB sticks) or third party hosting services (such as Google Mail) for high or medium risk personal data or business information.
 - g. Avoid sending high or medium risk personal data or business information by email. If you must use email to send this sort of data out with the University environment, encrypt it. If you are sending unencrypted high or medium risk personal data or business information to another University email account, indicate in the email title that the email contains sensitive information so that the recipient can exercise caution about where they open it.

- h. Do not use high or medium risk personal data or business information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high or medium risk personal data or business information to an insecure device.
- i. Consider the physical security of high or medium risk personal data or business information, for example use locked filing cabinets/cupboards for storage.
- j. Implement the University's retention and disposal policies so that you do not keep personal data and business information that you do not need. If there are no suitable retention and disposal policies in place for your area, arrange to put some in place.
 - <http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/RMguidance.htm#RetentionSchedules>
 - <http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/Retention/Retention.htm>

High risk personal data or business information

9. The following types of information are examples of high risk personal data or business information:
 - a. Any set of data relating to 1000 or more identifiable individuals, including but not limited to students, staff, alumni and research participants.
 - b. Any set of data relating to more than 50 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 more than 50 individuals' performance, grading, promotion or personal and family lives.
 - d. Information relating to more than 50 alumni/students' programmes of study, grades, progression, or personal and family lives.
 - e. Any set of data relating to 10 or more identifiable individual's health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.
 - f. Health records of any identifiable individual
 - g. Substantial reorganisation or restructuring proposals that will have a significant impact on more than 50 individuals before the decision is announced.
 - h. 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.
 - i. Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.

Medium risk personal data or business information

10. The following types of information are examples of medium risk personal data or business information:

- a. Any set of data relating to more than 50 but less than 1000 identifiable individuals, including but not limited to students, staff, alumni, research participants.
- b. Any set of data relating to 10-50 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 10-50 staff's performance, grading, promotion or personal and family lives.
- d. Information relating to 10-50 alumni/students' programmes of study, grades, progression, or personal and family lives.
- e. Any set of data relating to 5-9 identifiable individual's 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. Substantial reorganisation or restructuring proposals that will have a significant impact on 10-49 individuals before the decision is announced.
- h. Information that, if compromised, would disadvantage the University in commercial or policy negotiations.

Information provided to the University in confidence.

What help is available?

11. The University Records Management Section provides advice, guidance and training on data protection, records management and freedom of information issues. Much information is available on our website, or you can contact the Section by email:
 - <http://www.recordsmanagement.ed.ac.uk/>
 - recordsmanagement@ed.ac.uk
12. Your IT support service can advise on the options for the encryption of electronic information.

Author: IT Security Working Group
April 2010