Policy on Categorising and Protecting University Information Assets

1. Purpose of this Policy

1.1 The purpose of this policy is to advise employees about the University's grading structure for Information Assets, and how to protect those Information Assets in order to prevent data loss. The policy applies to all University Information and advises users on levels of security and encryption required on data held on all types of media and in hard copy.

1.2 This Policy clarifies and builds upon the Confidentiality Policy approved by Senate (*ref G/70/908*) in the early years of the University (which first adopted the Information Grades defined at 3.1) within the context of contemporary ICT and information legislation.

1.3 It should be noted that the Information Commissioner's Office (ICO)[1] has the power to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act, for example the loss of an unencrypted laptop containing the personal information of numerous individuals.

2. Key Objectives

2.1 The key objectives of this policy are to:

- define how to:
  - grade information correctly;
  - store and transfer information appropriately to its grade;
- prevent data loss or breach of information legislation due to inappropriate information storage and transfer.

3. Handling Information Assets

Information is an asset and needs to be handled appropriately to the information's grading.

3.1 *University Information Grade Hierarchy*

The process of assigning a grade is user-led; users assign their information assets to one of four grades.

---

1 https://ico.org.uk/

1. Personal data

Description: Personal information protected by the Data Protection Act. Access should be by relevant staff only and the information can be circulated to named recipients only. Any further distribution to be explicitly approved by the author and must represent permitted processing◊ under the Data Protection Act.

Examples: The personal data of students, staff and third parties including data held within filing and information systems, references and any documents or communications discussing individuals.

2. Restricted

Description: Information which is for circulation to named recipients only. Any further distribution to be explicitly approved by the author.

Examples: Senior management discussion papers, strategic development papers, items which are commercial in confidence.

3. Confidential

Description: Information of internal interest or being prepared for publication. Recipients may forward to others within the University.

Examples: Unpublished information, draft papers which do not fall into the Restricted or Personal categories.

4. Ordinary

Description: Information that has no constraints on its publication. No grade marking is required. Available to all including external parties.

Examples: University prospectus, external facing web-pages.

◊ Permitted processing and the Data Protection Act

Principle 2 of the Data Protection Act states that, 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'. Distribution is one example of processing.

Principle 8 of the Data Protection Act states that, 'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

3.2 *Relevant Legislation*

3.2.1 Freedom of Information Act (FOI)

Under the Freedom of Information Act, the majority of our information assets can be considered ***ungraded***. As our web page (https://www.lancaster.ac.uk/freedom-of-information/) states:

> "Lancaster University is legally required to answer all written enquiries and requests for information from any person or organisation in the world within 20 working days, subject to certain exemptions."

Whilst the use of a grading other than Ordinary is an indication that there may be an applicable exemption from disclosure under FOI, there is no guarantee that this is the case. Any use of a FOI exemption may be challenged and overturned by the Information Commissioner's Office.

3.2.2 Data Protection Act (DPA)

New penalties for serious data protection breaches have been recently announced by the Information Commissioner who can serve notices requiring institutions to pay up to £500,000 for serious breaches.

A serious breach is defined as a serious contravention of the data protection principles that was likely to cause either substantial damage or substantial distress. Additionally, this contravention would either have been deliberate or it ought to have known that there was risk and that there was a failure to take reasonable steps to prevent the breach.

Employees of the University need to be aware that this applies to all personal data[2] whether or not this has been formally graded.

3.3 *Information Security Hierarchy*

The grade assigned to the Information Asset, in conjunction with where it is stored, will define the level of Information Security required.

---

[2] All information from which it is possible to identify an individual is personal data. More detailed guidance on identifying personal data is available from the Information Commissioner's Office at: https://ico.org.uk/.

Grade	Information Asset	Hard copy	Asset on University's IT system	Asset on Mobile Device†	Email distribution	Grade marking
1	**Personal Data ≠**	Locked storage	Authenticated *	Encryption required	See Ω	Recommended ≠
2	**Restricted**	Locked storage	Authenticated *	Encryption required	Not recommended	Required
3	**Confidential**	Locked storage recommended	Authenticated *	Encryption recommended	Permitted	Required
4	**Ordinary**	Unsecured	Unauthenticated	Encryption not required	Permitted	Not required

Key

Action required	Action recommended	No Action required

***** Authenticated items require staff to supply credentials (such as University username and password) to access the data.

† These mobile devices may, or may not, have been provided by the University. For the purposes of this policy, mobile devices include, but are not limited to: Laptop PCs, Blackberries, Mobile Phones, USB memory sticks; and includes media such as CDs, DVDs, memory cards, and external hard disk drives.

Ω Whilst it is not recommended to distribute personal data by email, in some cases, for example when providing references, this may be considered necessary. The distribution of datasets containing the personal information of more than one individual by email should be avoided where practicable. Datasets containing the sensitive personal data of multiple individuals must never be distributed by email. ISS can provide advice on the secure transfer of such datasets.

Section 2 of the Data Protection Act defines Sensitive personal data as:

'information as to:

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the ***M1****Trade Union and Labour Relations (Consolidation) Act 1992),*
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.'

≠ Whilst documents containing personal data should be graded and marked, employees cannot rely on this to be the case and must take responsibility for identifying personal data and applying the appropriate level of security to all personal information which they process. It should be noted that datasets contained within information systems will often contain personal data which will not have previously been marked as personal.

4. Compliance

4.1 It is the responsibility of Departmental Heads to ensure that users within their department are aware of and follow this Policy.

4.2 **All members of staff** should be aware that they must:

- follow this policy;
- adopt the practices described within the Information Security Policy and Processes;
- report lost hard copies and mobile devices holding Restricted or Personal information immediately to the Secretariat and to the Chief Information Officer;
- remove copies of Restricted or Personal University information from personally-owned devices before leaving University employment.

4.3 In cases where it is essential to distribute graded items to external recipients, it is the responsibility of the **Distributor** to ensure that the **External Recipient** is made aware of, and agrees to, the restrictions imposed by this policy and the document's grade.

4.4 Failure to follow this policy may lead to disciplinary action and/or legal action being taken against those involved, which could ultimately lead to dismissal and/or criminal proceedings in the case of the loss of Restricted or Personal information.

5. Further Guidance on Information Security

5.1 Users should read this policy alongside the Information Security Policy and Processes which defines how the University manages its Information Security practices.

5.2 Advice on encryption may be sought from the ISS Service Desk.

5.3 The Strategic Planning and Governance Division's Compliance team can provide further advice on data protection and other information compliance and records management issues.