Loughborough University

Information Security

Information Categories and Controls Policy

Version 1.0:
Approved June 2016
Review May 2023

Information Categories and Controls Policy

1. Purpose

The right level of security can only be applied to information if those creating, storing, processing and potentially sharing the information are conscious of how sensitive and confidential the information is. To aid structured thinking about this issue and for use within other information security policies, a categorisation scheme for University information is set out below.

2. Scope

This policy is relevant to all staff, students and third parties that have access to University information and the relevant University information systems.

Given the volume of information held in the University, users are not expected to physically label all information with one of the Categories below. However, they are expected to be familiar with the Categories and to use them to inform their working practices. All Highly Confidential category information should be labelled as such given the need for extreme security measures for its handling.

3. Information Categories and Handling

The table sets out the information categories used at Loughborough University and the required approach to handling information in each category. The format in which the information is held may be electronic or hardcopy.

Category	Examples	Control Measures
1. Public **Available to anyone anywhere in the world regardless of their connection with the University**	Already published information (e.g. public University website): Prospectuses, newsletters etc. Charter, Statutes, Ordinances & Regs Most general policies & procedures Staff Research interests Open Access Research Data Job vacancies Contact details for public staff roles	Can be disclosed or drawn to the attention of anyone. For most purposes, the format should preserve the integrity of the information (e.g. share in PDF format rather than Word/Excel). However, open access research data will be made available in a readily analysable form (e.g Excel, .csv, Word or .txt) Contact details will be for specific public-facing roles only.

Category	Examples	Control Measures
2. Not Sensitive **Information which is not pro-actively published but which is not confidential or sensitive** **Can be shared openly amongst staff, students and third parties on request.**	Some internal procedural/operational Documentation Some Committee papers/review documents/discussion papers which are not openly published (especially after the elapse of time) Statistical reports where there are no competitive issues Internal non-confidential research reports	May be stored in any formats and systems which are efficient for the user/process concerned. If shared, the format should preserve the integrity of the information where appropriate (e.g. Marketing information/official institutional information should be shared in PDF format rather than Word/Excel). It would be good practice to seek the consent of the originator before circulating further.
3. Confidential **Unauthorised disclosure would cause a breach of legal responsibilities, financial and/or reputational damage to LU or to the individuals involved.** **May be shared internally and externally on a restricted and secure basis.** **This category includes most information defined as confidential in Section 27 of the Academic and Academic Related staff Conditions of Service - unless such information falls within the Highly Confidential category below.**	Personal staff and student data, including medical information, disciplinary information, PDRs, information on ethnicity or religion etc. This is referred to as 'Sensitive Personal Data' by the Data Protection Act (1998) Research data or other intellectual property covered by confidentiality agreements or with potential for commercial exploitation by LU (Theses, dissertations etc.). Commercial contracts or information relating to their negotiation. Sensitive policy/committee documents/correspondence (e.g. relating to major changes/new developments/discontinuation of activities, financial issues) Examination papers prior to examinations being taken.	Should be stored in secure, password protected and normally corporate IT systems (or locked locations if hardcopy) May be shared between authorised staff and students for legitimate business purposes. May be shared with third parties where appropriate permission has been given (personal data) or where covered by explicit agreements between relevant parties (e.g. research collaborations, funding bodies etc.) See further info on secure storage and information sharing in Staff Responsibilities and Information Sharing policies.
4. Highly Confidential **Exceptionally confidential information which would cause major financial loss, and reputational damage or significant distress to the data subject if used in an unauthorised manner.** **A very limited number of individuals will have access.**	Information obtained or generated through a partnership covered by the Official Secrets Act or a contract/partnership requiring extreme security measures (e.g. some NHS data).	A specific agreement will set out the individuals with access and will detail data storage, sharing mechanisms and working practices.