London Business School

Data Classification and Handling Policy

Audience: This document is for anyone who stores, handles, or processes London Business School information or data.

Document Owner: Data Privacy Manager / Information Security Manager

Release Date: v2.0, September 2023

Contents

1. Introduction

Information is a critical asset and fundamental to the School's mission to have an impact on the way the world does business through its teaching, research, and delivery of higher education (HE) related services. The School is committed to protecting and securely managing all its information and data assets, and this policy will help data owners, users, and processors to understand how to classify and handle information to support this.

The purpose of this policy is to detail the requirement for London Business School ('LBS' or the 'School') to protect information and data by ensuring it has a classification. Data classifications allow data owners, users, and processors to understand how to handle information in the most appropriate way and in line with the risks posed by its sensitivity.

This policy outlines the School's data classification scheme and the requirements for how each classification of information should be handled throughout the data lifecycle of creation, use and deletion once the information is no longer needed.

2. Scope

This policy applies to all types of information stored, processed, transmitted, or otherwise handled by the School, such as personal data, School Intellectual Property, research data, technical data, or financial information. There are no limitations to data types.

This policy applies to all formats. Data will be held on numerous formats such as personal workstations, servers, shared drives, laptops, USB keys and mobile devices. The scope of this policy applies to all digital information, including audio and visual data, and hardcopy data including printed materials such as reports and thesis papers.

This policy applies to all people that own, use and process data within the School such as faculty, staff, participants, students, and alumni, and anyone who is contracted by the School to provide services or handle School data or information externally.

3. Data Classification and Labelling Objectives

The following control objectives are relevant to data classification and labelling, and will be adhered to by the School:

- Information is classified according to the information security needs of the organisation and relevant interested party requirements.
- An appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by the School.

4. Data Classifications

Data classifications must be consistent with the School's requirements and consider data asset value and significance. The purpose of the classification scheme is to ensure information is labelled and handled in line with its sensitivity and the impact of loss or misuse of the data. Data classifications and the required handling practises apply by default but may be subject to amendment. Information may be disclosed via freedom of information or other legal or regulatory requirement in consultation with the School.

The information asset classification scheme shall be reviewed at least once a year or following any significant change to the School's business processes.

The following classification scheme applies to all School information. The classification levels are **Public**, **General, Confidential** and **Restricted**.

The following classification scheme applies to all School information:

London Business School Data Classifications:

Classification Level	Examples of Information
Public LBS information that is published for the public and/or could be disclosed with no risk.	• Website materials • Advertisements • External vacancy posts
General Non-public, LBS information that can be shared with internal employees, business guests and external partners. Unauthorised access, modification, or destruction, both internally and externally, would have limited impact on the School.	• General business process documentation • General School / business function announcements / communications • School standards and procedures
Confidential Non-public, sensitive, or valuable LBS information which can be shared with trusted recipients only. Unauthorised access, modification or destruction could adversely impact the School.	• Personal Data (as defined by the Data Protection Act 2018 (DPA)) • Vendor and supplier contracts • Human Resource records • Marketing and intelligence reports • Profit and loss information • Internal newsletters • Risk assessments • Risk register • Subject access requests (DPA) • IT / Systems documentation • Standards • Technical vulnerability assessments • Transaction records
Restricted Highly sensitive information including information with a commercial, legal, or regulatory impact. Can be shared with a restricted number of trusted recipients only. Unauthorised access, modification, or destruction, could significantly impact LBS, resulting in substantial damage to the organisation.	• Special Category Information (As defined by DPA 2018) • Personal Sensitive Information (Such as Criminal Record Information) • Application source code, particularly security functions • Student/employee bank and credit card details • Penetration test results and reports • Audit reports (both internal and external) • Documents relating to internal investigations or disciplinary action • School strategic plans • Intellectual property e.g., software code base, design plans, new products / services • Contracts with restrictions • Legal cases undergoing litigation • Sensitive financial information e.g., Annual Results prior to release • Audit reports (external and internal) • Security configurations and security audit log files • Encryption key algorithms and processes

5. Data and Information Handling Practises

Different classifications of data require handling practises that reflect the impact of its loss or misuse. The following practises are required to be followed to help reduce the risk of a data security incident.

Public information is not listed in the table below because there are no specific handling requirements for public information.

Area	General	Confidential	Restricted
Electronic Storage	Use approved cloud services and third parties that provide adequate security assurances and terms and conditions. Control access with network controls or controls at distribution list level. Restrict access to larger authorised groups or whole organisation.	Use approved enterprise cloud services with relevant contractual agreements. Control access via strong password authentication. Ensure two-factor authentication is enabled. Restrict access to authorised individuals or groups.	Use approved enterprise cloud services with relevant contractual agreements. Control access via strong password authentication. Ensure two-factor authentication is enabled. Restrict access to folders to specifically authorised individuals or groups.
File transfer	Transfers of data controlled using network controls or distribution lists.	Use approved cloud services (e.g., SharePoint) with authenticated access or collaborative folder invitation. Use secure transfer protocols.	Avoid transfers of data if possible. Ensure transfers targets are checked. Use Approved enterprise cloud services with authenticated access and collaborative folder invitation. Use secure transfer protocols.
Using email	Double-check recipient address. Use blind copy (bcc) when mailing large numbers of recipients.	Use content encryption when possible. Double-check recipient address. Use blind copy (bcc) when mailing large numbers of recipients. Encrypt attachments when sending to external recipients and share passwords separately via trusted means.	Use of email used only with explicit permission from data owner for file transfer and use of content encryption when possible. Double-check recipient address. Use blind copy (bcc) when mailing large numbers of recipients. Encrypt attachments when sending to external recipients and share passwords separately via trusted means.
Computers, laptops, tablets, and smartphones	Use LBS supplied and managed computers and laptops. Laptops should be secured at all times and locked away overnight when left in the office. Use non-LBS or personal devices in compliance with the Acceptable Use Policy.		
Removable Media	Non-encrypted devices permitted.	Encrypt devices and share passwords separately via trusted means.	Avoid downloading files to laptops and portable media but where this is not possible files should be retained only

			on a temporary basis and erased as soon as possible. Removable media should be secured at all times and locked away overnight when left in the office.
Post	Can be sent by any postal means.	Sealed envelope with sender details. Sent by recorded delivery or courier.	Sealed envelope with sender details. Sent by recorded delivery or courier.
Paper storage		Desks and offices in restricted-access premises. Locked draws, filing cabinets or equivalent in unrestricted-access premises.	Locked drawers, filing cabinets or equivalent in restricted-access premises or highly trusted third parties. Print only what is needed to hold as hard-copy and dispose of securely as soon as possible. Use only LBS printers.
Data Destruction	Erase or physically destroy if required. Shred paper documents.	Erase or physically destroy if required. Approved Third party data destruction services only. Shred paper documents using shredding equipment meeting DIN66399 P3 -P5 standard.	Erase or physically destroy if required. Approved third party data destruction services only. Shred paper documents using shredding equipment meeting DIN66399 P4 - P5 standard.
Generative Artificial Intelligence	Non-public data must not be entered into cloud-based services, including Large Language Models (LLMs) and AI chatbots, unless there is approval from the Data Privacy Officer.		

6. Data Labelling

Information and data can be labelled to automate data distribution and help consumers of data understand the risk applied to that data element.

The following labelling policy requirements are used at London Business School.

Classification	Labelling Requirements
Public	Label not required.
General	General by Default. No Encryption Required. Allow access to all users. Add General Header or Footer to all documents. Justification required to downgrade label.
Confidential	Manually label as Confidential. Apply encryption to documents and emails. Add a footer to all documents. Allow access to all users. Co-ownership assigned to all users.

	Justification required to downgrade label.
Restricted	Manually Label as Restricted. Apply encryption to documents and emails. Add a footer to all documents. Allow access to all users. Co-ownership assigned to all users. Justification required to downgrade label.

7. Roles and Responsibilities

Chief Digital and Information Officer (CDIO)

- The CDIO has accountability for Data Classification and Handling and must ensure compliance is met throughout the organisation with this policy.

The Data Privacy Manager / Information Security Manager

- The Data Privacy Manager and Information Security Manager will have joint ownership of this policy.
- The Data Privacy Manager and Information Security Manager are jointly responsible for ensuring that appropriate controls are defined and implemented, and that data classification and handling are coordinated and effective across the organisation.
- The Data Privacy Manager and Information Security Manager are jointly responsible for determining methods of implementing and monitoring, and for advising the business on data and information handling related issues.
- The Data Privacy Manager and Information Security Manager will ensure that data classification and handling awareness is increased, and compliance assurance is reported on regularly.

Data Privacy & Security Committee

- Led by the DPO and CDIO this is a multidisciplinary group that reviews, endorses, and supports the implementation of changes to the Data Classification and Handling policy and related documents and processes, as well as supporting data protection policies and requirements.

All LBS Employees, Faculty, Contractors, Students, Participants and Alumni

- All School Employees, Faculty, Contractors, Students, Participants and Alumni are responsible for complying with this policy.
- They are required to complete any data classification and handling training and are responsible for making informed decisions to protect London Business School's information and data assets.

8. Compliance and Exemptions

London Business School shall conduct appropriate compliance and assurance activities to ensure objectives are being met. Any violation of this policy will be subject to disciplinary action, up to and including termination of employment. Serious breaches may lead to criminal or civil proceedings.

Exemptions to this policy may be granted subject to the approval of the CDIO. All exemption requests shall be recorded along with their outcome.

9. Review and Continual Improvement

This policy shall be reviewed periodically by the DPO, CDIO and Data Privacy & Security Committee when there has been a significant change to the environment or business process to ensure that they:

- Remain operationally fit for purpose.
- Reflect changes in technologies or business processes.
- Are aligned to industry good practice; and
- Support continued regulatory, contractual, and legal compliance.

10. Document Control

Document Information

Title	LBS Data Classification and Handling Policy
Author	Information Security Working Group
Approver	Chief Digital & Information Officer; Data Privacy & Security Committee
Owner	Data Privacy Manager / Information Security Manager

Version History

Version	Date	Summary of Changes
Published	September 21	Approved and published policy
2.0	September 2023	Full policy refresh; updated classifications & policy template