UNIVERSITY OF LONDON

Data Classification Policy

1 Introduction and Scope

1.1 This policy aligns with the University's "Strategic Objective 3: *Developing and continuously adapting our organisation and capacity to anticipate the university of the future* - 3. Align our organisational structures and capacity to delivering our strategic aim and objectives".

1.2 The University stores and creates an extensive range of data sets in digital and hard copy format. These data sets hold varying risks and challenges for the University, requiring the prioritisation of resources and management.

1.3 The University is subject to a range of legislation for the management of personal data, financial information, and commercial records:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act (Section 46 Code of Practice for Records Management)
- Payment Card Industry Data Security Standard (PCI DSS)
- Prevent Duty
- Equality Act 2010,
- Protection of Freedoms Act 2012
- Counterterrorism and Security Act 2015

1.4 Breaches of the UK GDPR and Data Protection Act 2018 can result in enforcement action from the Information Commissioner's Office, including fines of up to £18m or 4% of global turnover.

1.5 The GDPR does not set specific security steps but requires 'appropriate technical measures' to be in place around data proportionate to the risk attached to it. A data classification scheme is a best practice technical measure to manage risk and allocate resources around datasets.

2 Policy Aims

2.1 This policy recognises data is an important asset for the University.

2.2 This policy recognises data classification is an essential approach to supporting effective management of risk and resources in implementing the University Strategy, with both business and compliance benefits.

2.3 All existing datasets in the University will be documented and classified according to the levels set out in section 3 below in a data asset register and given an owner with responsibilities set out in Section 4.

2.4 All new projects collecting data will have to classify the data they are collecting as part of the project.

2.5 Projects to develop and implement the classification policy will be supported by VCEG with appropriate resource.

3 The classification levels

3.1 This policy defines the 5 levels for classification as follows:

Proposed Classification	**Examples**
Highly Confidential	• ‘Special Category’ personal data as set out in the GDPR • Criminal convictions or offences data • Potentially offensive material • Disciplinary records for staff or student • Equalities and diversity data linked to individuals • Health and Safety / Sickness absence records.
Confidential	• Personal data • Company statistics or reports • Financial records • Restricted research data • Commercially sensitive information
General	• Teaching materials • Exam papers (post-examination) • Intranet posts with any attached documents • Anonymised or pseudonymised reporting
Public	• Anything cleared for public viewing (e.g., web content, press releases, social media posts)
Non-Business	• Non-business data (e.g., information falling under ‘reasonable personal use’ in the University’s Acceptable Use Policy)

3.2 The University will further develop and enforce its existing standards of data handling for each classification level relating to:

- Storage (e.g., penetration testing of IT system / database)
- Transfer (e.g., encrypted if sent via email)
- Access (e.g., multi-factor authentication)
- Disposal (e.g., secure deletion and evidence / record retained)

4 Responsibilities

4.1 **Vice Chancellor's Executive Group** (VCEG) - Accountable for governance and compliance at the University and responsible for:

- approving the data classification policy
- ensuring the proper implementation of this policy across the University
- ensuring adequate resources are in place to enact the requirements of this policy

4.2 The University's **Head of Data Protection and Information Compliance** (the University's statutory Data Protection Officer) is responsible for:

- drafting the data classification policy
- ensuring the data classification policy is kept up to date, is accompanied by appropriate formal procedural arrangements and is implemented across the University
- maintaining the University's Data Asset Register
- reporting on progress and escalates issues to the University Secretary and other channels as appropriate
- investigating and remedying any apparent non-compliance with this Policy at the University
- ensuring effective communication of the data classification policy, including for communicating changes to it
- ensuring appropriate training is provided to all staff, commensurate with their role and responsibilities, and for ensuring the training is evaluated and kept up to date

4.3 **Data Stewards** (all staff with responsibility for managing a dataset, such as a business owner or system administrator) are responsible for:

- Applying a classification to their data based on the criteria provided and providing it to the Head of Data Protection and Information Compliance
- Ensuring user access to 'highly confidential' and 'confidential' data sets are controlled and regularly audited

- Ensure all users are appropriately trained in using and accessing the dataset (in addition to essential data protection and IT Security training)
- Notifying the Head of Data Protection and Information Compliance if there is any unauthorised access of loss in relation to the data or any change or addition to the dataset which may require a change in classification level

4.4 **All staff** (includes all University staff, fellows, contractors, and any associated personnel acting as representatives of the University) are responsible for:

- ensuring they understand the data classification policy and how to operate within its remits and with the tools made available
- attending training relating to data classification as requested
- ensure new projects collecting data are notified to the Head of Data Protection and Information Compliance

5 Review

5.1 This classification policy will be reviewed as required by VCEG and on the recommendation of the Head of Data Protection and Information Compliance.

5.2 Reporting requirements on the policy will be developed by the University Secretary and the Head of Data Protection and Information Compliance, subject also the recommendations of VCEG.

6 Version Control

Date	Version	Purpose/Change	Author
July 2021	0.1	Initial draft updating previous Data Classification Policy and informed by comments from VCEG over initial data classification paper.	Data Protection & Information Compliance Manager
July 2021	0.2	Updated following review and comments by Director of Strategic Planning and Performance	Data Protection & Information Compliance Manager
August 2021	0.3	Updated following review and comments by Director of ITDS and Associate Director IT Security Business Continuity	Data Protection & Information Compliance Manager
September 2021	1.0	Approved by the Vice-Chancellor's Executive Group (VCEG)	Data Protection & Information Compliance Manager