Data Classification and Handling Policy

1. Introduction

1.1 What is classification?

1.1.1 Classification is the process of analysing and labelling data (digital, paper or otherwise) according to the impact a compromise of its confidentiality, integrity and/or availability would have on LSHTM. The greater the impact, the higher the classification. 4 Levels of classification are used by LSHTM: Public, Internal, Confidential & Highly Confidential.

1.1.2 This policy outlines types of data and provides instruction on the classification to be applied and how it may be handled.

1.2 Why must data be classified?

1.2.1 Without appropriate classification and labelling, data will likely be inconsistently managed. This inconsistency may lead to sensitive data being processed in inappropriate ways, potentially leading to a damaging data breach. A breach may result in unlimited fines and severe reputational damage.

1.2.2 Classification enables efficient processing of data. Often, most data organisations process is not highly sensitive. If data is not classified, it would be necessary to handle all data as if it was highly sensitive to comply with legal requirements. This results in restrictive protections, creating unnecessary demands to many common tasks. Unnecessary restrictions can slow and frustrate completing primary operational tasks. This unnecessary workload creates "friction" between the primary objectives of organisations and the secondary demands such as compliance. Too much friction and LSHTM is less likely to comply with policy. By appropriately labelling data in combination with controls selected to balance both data protection obligations and the need to reduce friction, greater compliance and security will be achieved.

1.3 Who must classify data?

1.3.1 Data owners are responsible for classification. Heads of departments and faculties are commonly considered data owners. It is their responsibility to discover and label information according to its sensitivity. However, data owners can be more broadly defined as those that create the data e.g. researchers collecting data in the field. Regardless all data owners must classify and appropriately label data according to LSHTM's Data Classification & Handling Policy.

Scope

2.1 Responsibilities

2.1.1 This classification policy applies to data for which you are responsible. Regardless of how the data is processed it must be classified.

2.2 Format

2.2.1 The classification considers information in terms of the degree of impact a compromise may have and not the form it takes. This includes but is not limited to digital, paper or verbal.

2. Disclosure

3.1 Freedom of information

3.1.1 This guide does *not* consider disclosure of information under legislation such as the Freedom of Information Act 2000. Any requests under this legislation should be transferred immediately to foi@lshtm.ac.uk.

3. Data Classifications

4.1 Public

4.1.1 Information that is produced for publication and/or could be disclosed with no impact on LSHTM can be labelled as Public. It is important to note that although the confidentiality of this category does not need to be maintained the integrity and appropriate availability must be. For instance, a press release on an emerging infectious disease is designed to reach a wide audience and so the confidentiality does not need maintaining. However, the integrity of the message is vital to maintain to prevent reputational damage. Availability in this instance is very important too. As if the data is not available the objective will fail.

4.2 Internal

4.2.1 Internal classified data can be characterised as non-sensitive, organisational data. If this level of data has any of its security properties violated it will have a low impact. Access is limited to members of the School and other authorised users. Disclosure may result in temporary inconvenience to individual(s) or organisation(s) or minor damage to reputation that can be recovered and has a small containment cost. Some common examples are: Project documentation, anonymised data that cannot be re-identified, organisational information that is appropriate for School staff and students only, staff training materials and non-sensitive committee minutes.

4.3 Confidential

4.3.1 Confidential data is the most common sensitive data processed. Access must be limited to specific named individuals. Disclosure may cause significant upset to individuals, reputational damage and/or financial penalty. Common examples may include interview notes, disciplinary correspondence, staff salaries, exam board minutes, datasets with sensitive personal data, student demographic details and assessments, staff appraisals and assessments, internal and external audit reports.

4.4 Highly Confidential

4.4.1 This highest level of classification is reserved for the most sensitive of data. Access to this data must be limited to specific named individuals having to work in an appropriately restricted manner. Compromised of this data may result in significant legal liability, severe distress/danger to individual(s), severe damage to organisational reputation and/or significant loss of asset value. Personal health data about identifiable individuals are a common example of this highly sensitive category. Personally, identifiable data shared with LSHTM by third parties such as the NHS and Personal health data about identifiable individuals collected by LSHTM staff and students are also in this category. NOTE: Data sharing agreements may stipulate processing requirements that fall outside of this classification and must be handled according to the agreement.

4. Data Classification and handling

	1-Public	2-Internal	3-Confidential	4-Highly Confidential
Classification description	Available to all	Available for LSHTM staff and other authorised users	Named individuals at LSHTM and/or collaborators	Named individuals only under strict controls
Level of risk if disclosed in error	None	Low	Medium	High
Examples	LSHTM Website. Any information within School's publication scheme. Publications. Press releases.	Information limited to School Internal policies and procedures	HR data, including recruitment materials for panels only. Sensitive personal data (as per DPA).	Research data that is personally identifiable (e.g. identifiable patient data) or can be linked with other data to become identifiable
Access control	No requirements	Authorised, individual account	Require specific controls	Require specific controls
Electronic storage				
Fixed equipment	No requirements	Access control & encryption	Access controls & encryption	Access controls & encryption
Mobile LSHTM devices	No requirements	Access control & encryption	Must not be processed without additional controls and approval from ITS.	Must not be processed on mobile devices
Personal Devices	No requirements	See BYOD Policy for standards required	Must not be processed on personal devices	Must not be processed on personal devices
Electronic Comms				
Email	No requirements	Consider recipients and limit circulation	Must be appropriately encrypted.	Must not be emailed
Fax	No requirements	Require recipient to be present	Fax not permitted	Fax not permitted

Voice mail	No requirements	Take care to ensure correct recipient	Not permitted	Not permitted
Independent file transfer	No requirements	LSHTM provided systems.	Must be appropriately encrypted. If relevant comply with additional obligations	File transfer not permitted
Paper				
Labelling	No requirements	No requirements	Label Confidential & enforce need to know	Label Highly Confidential & enforce need to know
Printing	No requirements	Collect printout immediately	No unattended and unauthenticated printing	Only on approved and "Highly Confidential" labelled printers.
Storage	No requirements	Clear desk policy	Locked in storage	Locked in secure storage
Posting	No requirements	Keep to intended audience, used sealed envelope	Registered post to be signed by name individual only	Approved, direct courier, signed by named recipient
Data owner review	Annual review - as per records management Procedure	Annual review - as per records management procedure	Annual review - as per records management procedure	Annual review - as per records management procedure
Disposal				
Paper	No requirements	Shred, fine crosscut	Shred, fine crosscut	Shred, fine crosscut
Electronic	No requirements	Secure wipe	Approved secure wipe	On-site, supervised secure wipe or degaussing