LSHTM Information Management and Security Policy

Supporting policy 9: Data Classification and Handling Policy

Approved by Management Board - May 2017
(edit for consistency and links to further information updated since)

1. Introduction

This policy is intended to help you protect the electronic information for which you are responsible. It applies to all types of information, such as personal data or research, teaching, audit or financial information; some or all of these may be held on personal workstations, servers, shared drives, laptops, USB keys and mobile devices.

Most of us keep a wide range of documents, images, presentations, artwork, technical specifications or software on our computers, which require differing minimum levels of protection from disclosure or damage. This policy will help you categorise your information and then think about the most appropriate ways of storing it to protect it against unauthorised access or use.

This classification relates to data for which you are responsible which may be held:-

- on devices and systems under your day to day management and custodianship;
- on servers or shared drives under the management of a database or system administrator. In this case, you will need to liaise with the administrator(s) about the sensitivity of your data; for example, there might be a need to set up separate servers/ partitions with different levels of protection if the same server is being used for data of widely differing sensitivities.

This guide does *not* consider disclosure of information under legislation such as the Data Protection Act 1998 or the Freedom of Information Act 2000. Any requests under this legislation should be transferred immediately to foi@lshtm.ac.uk.

The classification considers information in terms of the degree of sensitivity rather than their purpose or format, and maps these to one of four levels of sensitivity: Public, Internal, Confidential and Highly Confidential.

For portable devices such as laptops, mobile phones, tablets, PDAs and USB keys, consider the policy on remote working and think twice about whether you need to carry files of higher sensitivity around with you when you travel.

The first step in protecting information is to focus on the risk of disclosure or loss and the resulting consequences. As risk assessment is a specialised area, this policy outlines particular types of data and indicates the appropriate classification to be used.

Note that data that could be considered anonymous, may no longer be anonymous if it is in the hands of someone who has other data, the combination of which allows re-

identification. Also, certain types of data can effectively identify individuals - for example, postcode and date of birth is likely to be sufficient to enable individuals to be identified. There is detailed information on the Information Commissioner's website at https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

The appropriate ways of protecting your information, including storage, access and everyday handling are then presented.

2. Data Classifications

The sensitivity classification levels are described below and relate to particular protection measures defined later.

1-Public

Description: Information that is published for the public and/or could be disclosed with no risk.

Examples: Information for the Internet; information already available publicly; information suitable for inclusion in publications; materials about the School that are known to be public; some LSHTM policies and governance structure.

2-Internal

Description: Limited to members of the School and specific collaborators. Disclosure beyond this 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.

Examples: Project documentation; address books; anonymised data that cannot be re-identified; aggregated datasets; organisational information that is appropriate for School staff and students only; staff training records; some committee minutes.

3-Confidential

Description: Limited to specific named individuals. Disclosure beyond this will cause significant upset to individuals or is expected to result in containment costs and/or financial penalty.

Examples: 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-Highly Confidential

Description - Very rare - limited to specific named individuals having to work in a very restricted manner due to the risk of significant legal liability or severe distress/danger to individual(s) or severe damage to organisational reputation or significant loss of asset value.

Examples: Personal health data about identifiable individuals; staff bank details.

3. Data Classification and handling

	1-Public	2-Internal	3-Confidential	4-Highly Confidential
Classification description	Available to all	Available within the School	Named individuals in School and/or collaborators	Named individuals only under strict controls
Level of risk if disclosed in error	None	Low	Medium	High
Examples (see section 2 above for further 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 particular requirements	Require School login credentials	Require specific controls	Require specific controls
Electronic storage - **fixed equipment** - **mobile devices including mobile phones and tablets**	No particular requirements	No special requirements on fixed equipment Recommend to encrypt data or device - 2526 bit minimum	Access controls and recommend encryption - 256-bit minimum Encrypt data or device - 256-bit minimum - or do not sync to mobile device	Access controls and encryption (data or device) required - 256-bit minimum Must not be stored on mobile device
Electronic transmission - **email** - **fax** - **voice mail** - **file transfer**	No particular requirements	Consider recipients and limit circulation Do test fax and require recipient to be present Take care to ensure correct recipient Use secure transfer	Encryption advisable, else anonymise data - 256-bit minimum Do test fax and require recipient to be present Take care to ensure correct recipient and do not leave any details in voicemail Use secure transfer as per data transfer agreement (create one if this does not exist)	Encrypt if absolutely necessary to email - 256-bit minimum Fax not allowed Take care to ensure correct recipient and do not leave any details in voicemail File transfer not allowed

	1-Public	2-Internal	3-Confidential	4-Highly Confidential
Paper handling - **labelling**	No particular requirements	Consider labelling - "2-Internal (LSHTM only)"	Label - "3-Confidential" and give a list of people allowed to see.	Label "4-Highly Confidential" and give list of people allowed to see.
- **printing**	No particular requirements	Collect printout asap	No unattended printing - collect immediately	No unattended printing - collect immediately
- **duplication**	No particular requirements	Limited duplication	Limited duplication	Very limited duplication
- **storage**	No particular requirements	Clear desk policy - out of sight when not in use	Store in secured location	Store in secured location
- **transmission (posting)**	No particular requirements	Care to keep to intended audience - seal envelope	Consider secure postage.	Secure postage to named recipient only
- **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 particular requirements	Shred	Shred - cross-cut	Shred - cross-cut
- **electronic**		Secure deletion of electronic data	Secure deletion of electronic data	Physical destruction beyond ability to recover

For details of how to encrypt data, see

https://lshtm.sharepoint.com/Research/Research-data-management/Pages/encryption.aspx

For mobile devices, it is easiest to encrypt the device itself. For laptops, see the information relating to full disk encryption at the above link. For mobile phones and tablets, see Guidelines 4 and 5 at http://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security