Information Security Classification Matrix

Version Control

1. Full Document Number:	ISTGUI007
2. Version number:	3.0
3. Superseded version number:	2.0
4. Document owner job title:	Data Protection Officer
5. Department / function:	Information Services
6. Approved by:	Head of Information Services
7. Date of approval:	10/03/2021
8. Next review date:	10/03/2022
9. Date of Equality Impact Assessment:	Not applicable
10. Equality Impact Assessment Reference Number:	Not applicable
11. Does this policy apply to LSTM Group (LSTM and subsidiaries?)	Yes
12. Add document to external LSTM website?	Yes

This document is uncontrolled if downloaded or printed. Always view the current version of the document via the Knowledge Exchange Policy Hub. Approved documents are valid for use after their approval date.

Modifications from previous version of document

Version	Date of issue	Details of modification
1.1	Tbc	Transferred to the new template. Additions provided by Head of IT (Service Delivery).
1.2	Tbc	Additional amendments to section on drives following ICT Committee, 17/10/18.
1.3	Tbc	Clarification added to use of cloud services such as Dropbox (section 6)
1.4	Tbc	Further amendments following discussions with Chair of ICT Committee
2.0	15/05/2019	Amendments to definitions as suggested by Data Protection Officer & Group Legal & IP Advisor
3.0	30/03/2021	Conversion to new document template, inclusion of Data Protection Impact Assessment where risk register was previously mentioned, practical tips to help staff apply the classification levels. Modified layout to make more accessible.

Contents

1 Scope

This policy applies to all staff who use and create information in their role. All staff need a broad understanding of the document to appreciate the information and classifications they may encounter.

2 Practical tips for classifying information

These steps can make it easier to classify information:

1. Determine the classification

   Assess the information you are handling. The default is Internal. If it is less sensitive, downgrade it to Public. If it is more sensitive, upgrade and classify as Confidential.

2. Store according to classification. You can mark the classification of files clearly by:

   - Write the classification in the filename, such as the final publishable version of a blog could end PUBLIC
   - Write the classification in emails, such as CONFIDENTIAL in the subject line
   - Develop access controls with your colleagues e.g. password protection for confidential or restricted areas in S: drive

3. Protect the information throughout its lifecycle (e.g. from creation, to sharing and use, to disposal) as per departmental retention schedule.

3 How to Use the Information Classification Matrix

1. Use the Key at the top of the Matrix to identify which column covers the information / data you wish to handle.

   For example, let's say that you need to send the hard copy personnel file of a staff member to another person in the LSTM. You would look at the key in the Classification Matrix and see that as you are dealing with person-identifiable information you need to be looking in the "Confidential" column

2. Look down the Classification Matrix until you find the action that you want to take with the information.

   In our example this would be "Transmission by Post, Fax or e-mail", "Mail within the LSTM (i.e. between buildings)"

3. Look along the row until you get to the relevant column which lists what you must do.

In our example this would be the "Confidential" column where you would find that you must send the personnel file in a "Sealed inter-office envelope marked Confidential".

4 Key to the Classification Matrix

		Public	Internal	Confidential	Restricted
Key	Examples of information / data to be handled.	Brochures, News releases, Marketing materials.	Routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, non-personal data, internal policies and procedures.	Personal data (except that which is Restricted), financial data, purchasing information, vendor contracts.	Statutorily protected and sensitive information e.g. strategic corporate plans / financial information.
	The consequences if the information / data is mishandled.	None.	Unauthorised disclosure would not significantly impact LSTM, or any of its stakeholders or employees.	Unauthorised disclosure could result in significant adverse impact or penalties to LSTM, its stakeholders or employees.	Unauthorised disclosure likely to result in significant adverse impact, embarrassment or penalties to LSTM, its stakeholders or employees.

5 Definitions of terms used in the Key

Public	‘Public’ information can be disclosed or shared without any restrictions on content, audience or time of publication. This must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to edit that information, and who have successfully authenticated themselves to the appropriate computer system.
Internal	‘Internal use’ information can be disclosed or disseminated by its owner to appropriate members of LSTM, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

Confidential	‘Confidential’ information includes personal data as defined under the General Data Protection Regulation (GDPR) and other information which may be deemed sensitive. Examples of this could include information shared with a supplier which is “commercial-in-confidence”; information covered by confidentiality agreements or strategic developments and business opportunities which should not be released to a third party. The information will be classified as “confidential” by LSTM or a partner and its unauthorized disclosure or dissemination would result in financial or reputational damage to the School. In the case of a breach of the GDPR this could include fines of up to €20 million from the Information Commissioner’s Office. Other negative outcomes could include the revocation of research contracts and the failure to win future research bids. Only those who explicitly need access must be granted it; and only to the least degree to do their work (the ‘need to know’ and ‘least privilege’ principles). When held outside LSTM on mobile devices such as laptops, tablets, or phones, or in transit, ‘Confidential’ information must be protected.
Restricted	‘Restricted’ information requires the same protection as ‘Confidential’ information, but in addition, it is subject to further controls on access, such as only allowing valid logons from specialist staff. Data defined as special category within the General Data Protection Regulations would fall into this class. ‘Restricted’ information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted.
Secure area	An area not reasonably accessible to unauthorised persons or an area where the protected information is not unattended by an authorised person. Examples include: private offices, work areas monitored by a staff member or receptionist, most employee only areas.
Lockable enclosure	An area or enclosure requiring a keypad entry. Examples include: locking cabinets, drawers, desks and storage areas, private offices with locking doors.
Need to know basis	A staff member may only have access to that information which is necessary to do their job.

6 The Classification Matrix

1. Transmission by spoken word

	Public	Internal	Confidential	Restricted
Conversation / Meetings	No special precautions required.	Ensure that you are not overhead.	Private setting. Avoid public areas.	Enclosed meeting area. Public areas prohibited.
Telephone calls via Skype for Business	No special precautions required.	Ensure that you are not overhead.	Avoid proximity to unauthorised listeners. If using speakerphone or conference calling facilities, ensure you are in a secure area.	Avoid proximity to unauthorised listeners. Use speakerphone or conference calling facilities only in a secure area.
Mobile telephones	No special precautions required.	Ensure that you are not overhead.	Ensure mobile phone is digital and avoid proximity to unauthorised listeners.	Ensure mobile phone is digital and avoid proximity to unauthorised listeners.
Voicemail / answer services on mobile telephones	No special precautions required.	Ensure that you are not overhead.	Only leave name and contact details	Only leave name and contact details.

2. Transmission by post, messaging service or e-mail

	Public	Internal	Confidential	Restricted
Internal mail within LSTM.	No special handling required.	No special handling required.	Sealed internal envelope marked "Private & Confidential"	Sealed internal envelope marked "Restricted and Confidential". Notify recipient in advance.
Mail outside of LSTM	No special handling required.	2nd class mail. No special handling required.	2nd class mail. Marked "Private and Confidential" with return address on the envelope. Traceable delivery is preferred e.g. Recorded or Special delivery.	Marked "Private and Confidential". Traceable delivery preferred, e.g. Recorded or Special delivery.
E-mail within LSTM	No special handling required.	No special handling required.	Refrain from use of personal data. Use of email discouraged where practical.	Use of any personal data is prohibited. Use of e-mail strongly discouraged, unless encrypted.
E-mail outside of LSTM	No special handling required.	No special handling required.	Use of e-mail containing personal data prohibited unless encrypted or emergency. Use of e-mail strongly discouraged. Broadcast to distribution lists is prohibited.	Use of e-mail containing personal data prohibited unless encrypted or emergency. Use of e-mail strongly discouraged. Broadcast to distribution lists is prohibited.

Fax location	Not to be in an area accessible to the general public.	Not to be in an area accessible to the general public.	Not to be in an area accessible to the general public.	Not to be in an area accessible to the general public.
Use of a fax coversheet	Required	Required	Required + coversheet to the labelled “Confidential”.	Required + coversheet to the labelled “Confidential”.
Fax transmission safeguards	Reasonable care in dialling.	Reasonable care in dialling.	Telephone before transmission to ensure that recipient is waiting by the fax machine for the transmission. Subsequent telephone call to confirm successful receipt of the transmission.	Telephone before transmission to ensure that recipient is waiting by the fax machine for the transmission. Subsequent telephone call to confirm successful receipt of the transmission.

3. Internet and Intranet (Knowledge Exchange)

	Public	Internal	Confidential	Restricted
	Content must be authorised by Head of Department of Group, or only added by authorised content creators.	Content must be authorised by Head of Department of Group, or only added by authorised content creators.	Must not appear on intranet / internet.	Must not appear on intranet / internet.

4. Storage media (including laptops, smartphones, memory sticks, networked drives, etc.)

	Public	Internal	Confidential	Restricted
	No special handling required.	No special handling required.	Use of personal data prohibited unless encrypted or an emergency.	Use of personal data prohibited unless encrypted or an emergency. Notify recipient in advance.
P: Drive **Assigned drive for personal / private use**	Permitted	Permitted	Permitted If the data is to be shared you must store this information in specific folders on to the S: drive	Permitted If the data is to be shared you must store this information in specific folders on to the S: drive

S: Drive **Assigned drive for shared: departmental use, for general document / file sharing and collaboration.** **private/ confidential documents (stored in specific folders and restricted to specific groups/ users within a department)**	Permitted	Permitted	Permitted Store only in specific folder that have been restricted to those staff members /students allowed to access the information Certain types of information such as Disciplinary proceedings etc. If you must store this type of information on a shared drive, consider encrypting the file	Permitted Store only in specific folder that have been restricted to those staff members /students allowed to access the information Certain types of information such as Disciplinary proceedings etc. if you must store this type of information on a shared drive consider encrypting the file
R: Drive **Assigned drive for research data.**	Permitted	Permitted	Permitted Store only in specific folder that have been restricted to those staff members /students allowed to access the information Certain types of information such as Disciplinary proceedings etc. If you must store this type of	Permitted Store only in specific folder that have been restricted to those staff members /students allowed to access the information Certain types of information such as Disciplinary proceedings etc. If you must store this type of information on a shared drive, consider encrypting the file

			information on a shared drive, consider encrypting the file	
Personal laptops/computers	Permitted data stored on the C: drive is not backed up and stored at the individual's risk	Permitted data stored on the C: drive is not backed up and stored at the individual's risk	Not permitted	Not permitted
Department owned servers and storage devices	Permitted	Permitted	Only permitted if: The server /data store meets LSTM's security assessment for IT systems and services Information is stored in restricted folders and where required files are password protected.	Only permitted if: The server /data store meets LSTM's security assessment for IT systems and services Information is stored in restricted folders and where required files are password protected.

5. Electronic file transfer

	Public	Internal	Confidential	Restricted
	No special handling required.	No special handling required.	Use of personal data prohibited unless encrypted (i.e. using SFTP, FTPS or secure VPN) or a one-off emergency.	Use of personal data prohibited unless encrypted (i.e. using SFTP, FTPS or secure VPN) or a one-off emergency.

6. Web portals including SharePoint, DropBox.

	Public	Internal	Confidential	Restricted
	No special handling required.	No special handling required.	Use of personal data prohibited unless encrypted (i.e. using HTTPS).	Use of personal data prohibited unless encrypted (i.e. using HTTPS).
LSTM provided cloud storage (DropBox for business, OneDrive, NextCloud)	Permitted	Permitted	Acceptable if documented within Data Protection Impact Assessment and discussed with the Data Protection Officer	Acceptable if documented within Data Protection Impact Assessment and discussed with the Data Protection Officer
SharePoint Online	Permitted	Permitted	Acceptable if documented within Data Protection Impact Assessment and discussed with the Data Protection Officer	Acceptable if documented within Data Protection Impact Assessment and discussed with the Data Protection Officer

Cloud Storage not provided by LSTM such as iCloud, GoogleDrive, Yammer, personal Dropbox, personal OneDrive etc.	Permitted	Permitted	Not permitted	Not permitted

7. Print images, Film, Fiche, Video, DVD

	Public	Internal	Confidential	Restricted
Printed materials	No special handling required.	Store out of sight of non-employees.	Store out of sight in a secure area.	Enclosed meeting area. Public areas prohibited.
Sign-in sheets or logs	No special precautions required.	Placement out of sight of non-employees.	Subsequent signers cannot identify previous signatories.	Subsequent signers cannot identify previous signatories.
Monitors / Computer Screens	No special precautions required.	Positioned or shielded to prevent viewing by non-employees.	Positioned or shielded to prevent viewing by unauthorised parties. Physical location in a secure area, positioning of screen, use of password protected screen saver etc.	Positioned or shielded to prevent viewing by unauthorised parties. Physical location in a secure area, positioning of screen, use of password protected screen saver etc.

8. Copying standards

	Public	Internal	Confidential	Restricted

	No special precautions required.	No special precautions required.	Photocopying to be minimised and only when necessary.	Photocopying can only be done with approval from the owner of the information.

9. Storage standards

	Public	Internal	Confidential	Restricted
Print material	No special precautions required.	Reasonable precautions to prevent access by non-employees.	Storage in a secure manner (e.g. secure area, lockable enclosure)	Storage in a lockable enclosure.
Electronic Documents	No special precautions required.	Storage on non-public drives only.	Storage on secure drives. Storage on shared drives without password protection for reading is prohibited.	Storage on secure drives only. Password protection of document preferred.
E-mail	No special precautions required.	Reasonable precautions to prevent access by non-employees.	Storage in a secure manner (e.g. password access or reduce to written form and store in accordance with storage of printed materials).	Reduce to written form if necessary secure manner or store in a lockable enclosure.

10. Destruction standards

	Public	Internal	Confidential	Restricted
Location of waste paper bins	No special precautions required.	Secure areas not accessible to unauthorised persons.	Secure area not accessible to unauthorised persons	Secure area not accessible to unauthorised persons.

Paper recycling	No special precautions required	No special precautions required.	Prohibited, unless by special recycling programme for confidential information	Prohibited. Destruction or shredding required.
Magnetic media / diskettes	No special precautions required	Overwrite or low-level reformat.	Overwrite or low-level reformat.	Overwrite or low-level reformat.

11. Physical security standards

	Public	Internal	Confidential	Restricted
Computers / Workstations	Password protected screen saver to be used when briefly unattended. Signoff or power off workstations or terminals when not in use or leaving work area.	Password protected screen saver to be used when briefly unattended. Sign-off or power off workstations or terminals when not in use or leaving work area.	Password protected screen saver to be used when briefly unattended. Sign-off or power off workstations or terminals when not in use or leaving work area.	Do not leave data unattended. Sign-off or power-off workstations or terminals when not in use or leaving work area.

Printing documentation	No special precautions required	No special precautions required	Printing of documents minimised and when necessary only. Unattended printing is permitted only if physical access is used to prevent unauthorised persons from viewing the material being printed.	Printing of documents when necessary only. Printers must not be left unattended. The person attending the printer must be authorised to examine the information being printed.
Office access	No special precautions required.	No special precautions required.	Access to areas containing sensitive information should be physically restricted. Sensitive information must be locked when left in an unattended room.	Access to areas containing sensitive information should be physically restricted. Sensitive information must be locked when left in an unattended room.
Laptops, tablets & other mobile devices	Password protected screen saver to be used when briefly unattended. Signoff or power off workstations or terminals when not in use or leaving work area. Also, laptops/mobile devices must be left unattended	Password protected screen saver to be used when briefly unattended. Sign-off or power off workstations or terminals when not in use or leaving work area. Also, laptops/ mobile devices must be left unattended or in motor vehicles	Computers must not be left unattended at any time unless the confidential information is encrypted.	Computers must not be left unattended at any time unless the confidential information is encrypted.

	or in motor vehicles			

12. Other actions

	Public	Internal	Confidential	Restricted
Access Control	Available to the public.	Generally available to all staff on a need-to-know basis.	Must have a business need to know the information. Must have written approval of the data owner.	Must have a business need to know the information. Must have written approval of the data owner.
Audit	None	None	Access should be audited as determined by the data owner.	Access should be audited as determined by the data owner.