Information Sharing Policy: Quick Guide

As a valuable component of University business, it is important we all understand our responsibility to use and protect information responsibly. Being able to share information and collaborate on ideas using accurate information is essential for the smooth operation of the University, whether it be internally between staff, between staff and students, or externally with partners. Information sharing takes place as a regular exchange of data, as part of automated processes, or as a one-off activity in response to a situation.

To support all members of the University to protect information, it has categorised information into four levels of sensitivity. It is important when preparing to share information to consider; **how 'sensitive' is the information you wish to share? If it was lost or ended up in the wrong hands what potential impact would it have.**

PUBLIC	NOT SENSITIVE	CONFIDENTIAL	HIGHLY CONFIDENTIAL
Available to everyone.	Can be shared openly amongst staff, students, and third parties on request.	May be shared internally or externally on a restricted and secure basis. Unauthorised sharing would cause individual, legal, financial or reputational damage.	Access very restricted. If used unlawfully would result in major financial and reputational damage, and/or significant distress to individuals or communities.
e.g. published information, prospectuses, staff research interests, job vacancies.	e.g. some internal procedures, some committee papers.	e.g. research data, commercial contract, personal student and staff data, negotiations, examination papers.	e.g. Information covered under the Official Secrets Act or Special Category information such genetic or biometric data.

Once the sensitivity level of the information is confirmed and before sharing, clarify:

- The safest and most appropriate method of sharing the information,
- That the recipients, recognise the information's' sensitivity and have made necessary preparations to protect and manage it from receipt through to deletion,
- With IT Services if you have any concerns about encrypting confidential information or best way to secure the information being shared, and
- The Data Owner has been consulted if confidential information is being shared and put in place any additional security measures needed.

Sharing Confidential or Highly Confidential Information

The following information provides guidance on sharing Confidential or Highly Confidential information using a variety of popular methods.

It is good practice to keep a record of any Confidential or Highly Confidential information sharing with external organisations or individuals.

You must tell the University IT Services if any device used to share information is lost, damaged, or stolen. If, you believe that the information you have shared has been compromised, used without authorisation or lost you must contact your Data Co-ordinator or the data protection team immediately.

If you need to share Confidential or Highly Confidential Information….

Method	Recommended	Risks	Solutions
Hardcopy (e.g. paper documents)	No	Easy to copy and share onwards without any control. Cannot be updated so can become inaccurate very quickly. Documents containing confidential information need to be disposed of securely in confidential waste bins.	If you need to share information in hardcopy, make sure the recipient understands what and how they are expected to keep, use, and dispose of the information safely.
Electronic	Yes (with care)	It can be easy for recipients to share electronic information onwards. Poor version control can lead to confusion and increase the risk of inaccurate information being used in decision making. Over-sharing increases the risk that information is stored in multiple places and kept for longer than is appropriate.	Before you share. Select a safe way to transfer the information and specify how it will be done. Only share when it is necessary and always try to use University systems. Rather than remove data from a secure corporate system. Provide time-limited. restricted access, for only named individuals to carry out specific tasks. Sharing information using Office 365 Groups or Group Workspaces helps to control access and prevent the creation and storage of multiple copies. If you must share information using a non-supported system, check first with the Data Owner and get confirmation the system complies with GDPR requirements; how will they store the data, Do they have a Data Protection Officer, is there a central record of data they hold, what security procedures do they follow, how do they manage access to data.
Email & Email Attachments	Yes (with extreme care)	There is a high risk that information could be lost, accessed, or shared with people who are not authorised to see it. Easy to forward on without any control. Can be easily mis-sent to incorrect email address. Kept in unstructured system, if not transferred to a file plan and could be lost.	Information should be made available internally using Office 365 groups or Group Workspaces. Confidential information should not be shared within the University using email attachments. If you need to use email to send information outside of the University, you will need to complete a Data Privacy Impact Assessment approved by a senior member of staff or committee. The information should be password encrypted, the password should be provided separately and not by email. If information must be sent externally using an email attachment. A disclaimer should be added to the message to alert the recipient of their responsibility to protect it.

Method	Recommended	Risks	Solutions
Cloud service e.g. One Drive and Working Groups	Yes	Office 365 makes it easy to store, share, and collaborate on documents. Take care to manage membership and access to working groups to avoid over-sharing and when staff change roles within the University. Access to working groups need to be maintained to ensure information doesn't become 'stranded' if the group owner leaves.	Decide which One Drive is recommended for making information you are working on individually available to others for a short period. Working Groups allow you to easily collaborate and maintain information with others. For more information go to: www.lboro.ac.uk/it/staff/storage/o365groups/ or email, it.services@lboro.ac.uk
Mobile/Removable storage & devices e.g. memory cards, USB drives, tablets, external hard drives	No (use with extreme care)	Small removable storage devices can be easily lost or left behind in public spaces. Data held on mobile storage devices can be easily accessed by others. Some devices are attractive to thieves. More vulnerable to hackers or viruses if used in multiple /public machines. Unsuitable as a permanent storage solution. If the device is lost or the encryption password forgotten, the information will be permanently lost. Very few camera media cards allow data to be encrypted	You will be responsible for the safety of information shared in this way. Ensure data held on the device is encrypted. If you must send or take a mobile / removable storage device off campus. Check first with the Data Owner and contact IT services to ensure the right level of security is in place. If the device is lost, damaged, or stolen inform IT Services immediately. Once the information has been shared, it must be deleted from the device. If the information must be posted, only use a service that tracks and guarantees delivery. Never include the encryption password together with the device. If you are using your own device/storage to access or share University owned information, IT Services can remotely wipe the device if it becomes lost, damaged, or the University is concerned it has been hacked / infected with a virus.