Loughborough
University

Information Security

Information Sharing Policy

Version 1.1:
Approved March 2019
Review June 2023

Information Sharing Policy

1. Policy Overview

The work of the University requires the sharing of information between staff, between staff and students, and between staff and (external) third parties. Seeking to maintain the open nature of the organisation, whilst also minimise the risk of loss, unauthorised disclosure, modification or removal of information maintained by the University; this policy section aims to provide members of the university clarity on sharing information in a safe and secure manner. This policy covers information categorised as Confidential under the University's Information Categories and Controls Policy. Examples include, personal staff and student data, research data and intellectual property covered by confidentiality agreements, commercial contracts, sensitive policy/committee documents, and examination papers prior to examinations.

2. Policy Audience

This policy applies to all members of staff, students and third parties who have access to Loughborough University information.

3. Scope

This policy covers the sharing of information, which has been categorised at different levels under the University's Information Categories and Controls Policy, and the mechanisms used to share such data. It covers all forms of information, whether held and shared in hardcopy or electronic format.

Routine sharing of information happens regularly as part of day to day activities at the University. Examples include circulating and/or providing access to documents via workspaces (i.e. job application packs, meeting packs) or sending general emails. In these cases, information may ultimately be accessed both via University owned and non-University owned/maintained electronic devices (please see below). This policy is not limited to routine activities and includes data sharing processes such as:

- Research data shared with colleagues both internal and external to the University (third parties) as part of a collaboration or agreement
- Information shared with the police in response to a legitimate request (i.e. under GDPR and the Data Protection Act).

Information sharing may also happen as part of automated IT processes and the process owner is responsible for ensuring the sharing complies with the guidance within this policy document.

4. General Guidance

Staff should be mindful to ensure they are handling information and applying appropriate safeguards in accordance with the Information Categories and Controls Policy.

Draft documents should normally be considered as ‘Confidential’ until they have been finalised or approved through the relevant line management or governance arrangements.

A flow sheet has been developed to help individuals make informed decisions when considering the sharing of information, t is the responsibility of those releasing the information to ensure that the recipient understands the confidentiality of the information and will abide by the provisions of this policy.

The remainder of this policy relates to the sharing of Confidential information.

5. Data Owner

All information within the University should have a Data Owner. The Owner is responsible for risk management and it is therefore the responsibility of the Data Owner to assign this information to a category (as per the Information Categories and Controls Policy), and provide advice and guidance on how the information should be accessed or shared, in accordance with the overarching Policy Framework. Being the Data Owner is not the same as being the owner of the Intellectual Property. Similarly, the Intellectual Property in the information may be held by someone who is not the Data owner. All staff should be aware of their individual responsibilities for handling data in the four categories above.

Examples of data owners:

- An individual with overall accountability to the organisation for an area of institutional data (e.g. Staff, Students, etc.)
- A document created by a member of staff on an aspect of their job for their own use. The data owner of this document is the member of staff who created it;
- Principle Investigators (PI) on research projects are the Data Owners of research data created or collected during the project.
- The data held within LUSI (student records system). The data owner for this data is the Academic Registrar;
- The data held within Agresso (finance system). The data owner for this data is the Director of Finance;
- Research data provided to the University by an external body. In the case of research projects, data may be shared or transferred with or from external bodies, and the rules governing the ownership, sharing or transferring will be determined by the Research Collaboration Agreement.

In some cases, it is possible that the data owner may delegate this responsibility to other members of staff, ultimately, they remain the data owner.

Individuals or groups analysing, or otherwise, making use of (including publishing) information categorised as ‘Not Sensitive’, ‘Confidential’ or ‘Highly Confidential’ must ensure they have the permission of the Data Owner in advance. This permission may be clear through standard working practices or through the agreements in place related to specific projects. However, it must be sought on a case by case basis when any unusual or non-standard use is to be made of University information. If ownership is not clear, this should be referred to the Information Governance Sub-Committee for guidance.

6. Sharing in Hardcopy Format

Sharing of Confidential Information in hardcopy form is discouraged as further sharing by the recipient remains easy and there is considerable risk of this information not being maintained or disposed of securely. If such sharing is undertaken, checks should be made on the arrangements for appropriate storage and disposal, and these should comply with the relevant University policies. For example, policy on the Management of User Access Information, and the University Records Retention Schedule.

7. Sharing in Electronic Format

Information is most frequently shared in electronic format. Such formats make information easy for recipients to share, potentially when it is not appropriate to do so. Over-sharing and informal arrangements for version control increase the risk that information will be stored in multiple locations, in different versions, and retained for longer than is appropriate.

Where Data Management Plans (DMPs) are written and/or ethics committee approval is sought, the responsible investigator should state clearly the proposed mechanism for sharing electronic data as outlined in this policy to minimise data loss or inappropriate sharing.

To minimise the risk of losing Confidential information, all members of the University should share content, only when required, using University provided systems, unless explicit approval for an alternative has been given.

Confidential information held in secure corporate information systems (e.g. LUSI, Co-Tutor, and iTrent), where access is managed and restricted to essential users, should not be removed from the controlled environment, except in instances where there are no other options available. To share confidential information with other individuals, where it is not supported by a corporate information system, the use of the Office 365 Groups or Group Workspace service with appropriately controlled access, is required. Sharing through this mechanism restricts access and removes the risks associated with creation of multiple copies.

Where sharing is necessary with external partners, corporate systems provided by the lead organisation should be used, otherwise explicit approval for an alternative should be sought. If Loughborough University is not the lead organisation, and personal information will be shared, the Loughborough staff member should seek explicit assurance that the system is GDPR compliant.

Email

As with other forms of electronic format, care should be taken when sharing information via email. This policy acknowledges that sharing Confidential information between University staff and students is essential for the conduct of day to day activities.

If it is essential to send confidential information via an email, or email attachment, to email addresses outside of the University, the potential risks to the security of the data should be considered and where proportionate a Data Privacy Impact Assessment (DPIA), should be undertaken to mitigate against possible data loss. Once shared, copies of documents will no longer be held within a corporate information system (e.g. a document is no longer situated within Office 365 Groups, Group Workspace, or the University's email system) and therefore can no longer be deemed secure. Information shared in this way is considered at high risk of being lost, compromised, accessed or shared with unauthorised individuals.

Where it is essential for the conduct of University business to share confidential information externally via email, it is recommended that a password is used to encrypt the Microsoft Office or Adobe PDF document and a suitable disclaimer included in the email:

"This message (including any attachments) may contain confidential, proprietary, privileged and/or private information. The information is intended to be for the use of the individual or entity designated above. If you are not the intended recipient of this message, please notify the sender immediately, and delete the message and any attachments. Any disclosure, reproduction, distribution or other use of this message or any attachments by an individual or entity other than the intended recipient is prohibited."

All users are advised to follow the steps identified in the 'Email Good Practice' document.

Cloud Services

The use of cloud-based storage makes collaboration and sharing of information very easy and convenient. The University has made a strategic decision to standardise on Microsoft Office 365 (including OneDrive and Groups) as the default cloud office collaboration platform for the organisation.

If there is any doubt about using any other service, advice should be sought from IT Services.

Other Electronic Media

The use of other electronic media other than Office 365 Groups and Shared Workspace service for sharing Confidential or Highly Confidential material is discouraged as they increase the risk of inappropriate sharing or loss of Confidential information. However, the use of such media is not prohibited as there may be no other option for very large data sets.

Mobile/Removable Storage and Devices

These are defined as all types of electronic storage which are not physically fixed inside a computer or laptop; or the device itself is easily moved. They include the following:

- Memory cards (like those used in cameras), USB pen drives etc.;
- Removable or external hard disk drives;
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player);
- Optical disks i.e. DVD and CD;
- Floppy disks;
- Backup Tapes.

If saving and sharing information via one of the above media is considered to be essential as it is deemed to offer significant advantages over use of one of the previously recommended, more secure approaches, the user must ensure:

- That anti-virus software is present and up to date on machines which data is taken from and machines which data is transferred to;
- All data is held on encrypted mobile/removable storage and devices at all times.

Information on anti-virus software and encryption of information can be found at:

- Staff: anti-virus
- Student: anti-virus
- IT Operations: Encryption Policy

Users wishing to transport and/or share Confidential information using electronic media MUST also ensure:

- The data on the device is encrypted to the highest recommended encryption standard (AES-256). Please contact IT Services for further assistance;
- Compliance with any certified level of encryption required under a research or other grant or contract (e.g. to a standard such as FIPS-140-2). If such requirements are stipulated, please contact IT Services for further assistance;
- Mobile devices and/or electronic storage devices containing Confidential information should not be sent off site without the prior agreement of the data owner. IT Services should be consulted to ensure the level of security is appropriate for the type of data being transferred;
- Electronic media used to store Confidential information shall only be used by authorised individuals and where there is a clear business need;
- Data stored on the electronic media is the responsibility of the individual who operates the device.
- That electronic media should not be used to store information which is not securely backed-up in a central location as should the encryption password be forgotten; the information will be irretrievable.
- That the electronic media is physically protected against loss, damage, abuse or misuse when in use, storage and transmit.
- That should any electronic media holding confidential information become damaged, it should be given to local IT Support or IT Services staff for secure disposal.
- That the University (IT Services) is notified in the event that the device is lost or stolen.
- That when the business purpose has been satisfied, the information is securely removed/deleted through a destruction method that makes the recovery of data impossible.
- .

Where electronic media containing Confidential information needs to be posted to third parties, services that provide tracking and auditing must be used. The decrypting password should not be in the same package as the media in question. Passwords should normally be provided to third parties either in person or via a telephone call.

In the event that a personally owned device is used to access or share University owned information, then the University reserves the right to remotely wipe the device in the event that it becomes damaged, lost or the University becomes concerned that the security of the information has been compromised. (Also see policy on Mobile Working).

Document Control

Version	Author	Date	Version Detail
V0.1	Niraj Kacha	22nd May 2015	First draft
V0.2	Jennifer Nutkins	18 Jan 2016	Revised following IGSC and including JCN amendments
V0.3	Niraj Kacha	18 Jan 2016	Major revision of Cloud Services section, flowsheet added, plus other minor amendments.
V.04	Jennifer Nutkins	23 Jan 2016	Incorporation of revisions and initial preparation for ITGC
V0.5	Niraj Kacha	11 Feb 2016	Minor changes following ITGC recommendation
V0.6	Mark Lister	February 2016	Minor changes following ITGC recommendation
V0.7	Matthew Cook	19th Feb 2016	Changes following IGSC recommendations
V0.8	Matthew Cook	9th Mar 2016	Changing following IGSC recommendations
V0.9	Jennifer Nutkins	21 Mar 2016	Further amendments to ensure relevant to all staff
V0.10	Mark Lister	15 April 216	To incorporate minor amends re: Research data owners and need to seek advice when data is leaving EU
V0.11	Matthew Cook	20th April 2016	Changes following ITGC recommendations
V0.12	Mark Lister	10 May 2016	Amends to wording
V0.13	Mark Lister	25 May 2016	To incorporate feedback and comments from ITGC and amends suggested by IGSC
V0.14	Mark Lister	26 May 2016	To incorporate feedback from JCN
V0.15	Matt Cook	2nd June 2016	Corrections and suggestions from ITGC.
V0.16	Mark Lister	13 June 2016	To incorporate suggestions by Peter Townsend and Gareth Cole
V0.17	Mark Lister	14 June 2016	Amendments to the Data Owner section.
V0.18	Mark Lister	14 June 2016	Further amendments to the Data Owner section.
V0.19 and V.0.20	Matt Cook and Mark Lister	26 November 2018	To update document following the publication of the Dropbox guidance.

V0.21	Claire Vallance, Gareth Cole, Mark Lister, and Matt Cook	29th January 2019	To include more clearly defined references to Research and Ethics processes. Policy to incorporate risk, authorisation, and possible enforcement.
V0.22	Claire Vallance	29th January 2019	To accept changes agreed between MC, GC and CV.
V0.23	Claire Vallance	14/03/2019	Alterations prior to presentation to ITGC.
V1.0	Claire Vallance	25/03/2019	Approved by ITGC subject to completion of a Quick Guide to the Information Sharing Policy.