Information Protection Guide

Introduction

As a University we share, collaborate on and manage information. Information that is essential for the day-to-day operations of a University, including: research; teaching; knowledge exchange; administration; partnership; and community work. It is important that all members of the University (students, researchers, staff, honorary members and third parties carrying out a University function) understand how they can support effective collaboration at the same time as protecting our (and our partners') valuable and sensitive information.

Classifying information helps you focus your effort and resources to protect the most sensitive and valuable information. The higher the risk of compromise, the more protection is necessary. Classification and proportionate protection measures will help to reduce the likelihood and impact of loss, misuse or compromise of the confidentiality, integrity and availability of the information. At the University of Liverpool, we use the following classifications:

Public	**Internal** (default)	**Confidential**
Information intended for sharing in the public domain **Impact if breached:** No adverse impact	Information used for day-to-day University functions, not for general public **Impact if breached:** Some adverse impact and disruption to services; possible breach of confidence or statutory duty	Any quantity of personal data (info about living people) or information with contractual, business or research value **Impact if breached:** Serious privacy or reputational risk, financial impact, commercial disadvantage or disruption to services Breach of statutory/regulatory duty/risk of fine

Follow the steps in this Guide to classify and protect University information

Step 1: Decide the classification. Use the definitions and examples to assess and decide the type of information you are handling. The default category is **Internal**. If less sensitive, downgrade it to Public; if more sensitive, upgrade it to Confidential.

Step 2: Store according to classification

Step 3: Protect the information throughout its lifecycle (from creation through sharing to disposal). Protection is cumulative so Confidential requires the Internal protection measures **and** requires extra protection.

Accountability and exceptions: There may be limited circumstances where the Data Owner (Principal Investigator, Supervisor or Head of Department/Institute) has a requirement to store classified information differently, or with increased safeguards, to the protection measures in this Guide. The Data Owner is responsible for documenting and managing the information risks and safeguards to comply with relevant legislative, regulatory and contractual requirements. For example to comply with Government (HMG) Policy.

Step 1: Decide the classification of the information you're handling

	Public Information intended for sharing in the public domain	**Internal** (Default - most information is internal) Information used for day-to-day University functions (accessible to most staff or students) not for general public	**Confidential** Any quantity of Personal data (living people), or info with contractual, business or research value Limit access to least number of people necessary
Impact if lost or compromised	No adverse impact	Adverse impact and disruption to operations/services Loss of confidence; breach of statutory duty	Serious privacy/reputational risk, financial impact, commercial disadvantage or disruption to services Breach of statutory/regulatory duty; risk of fine
Examples	• Annual reports and publications • Course and contact information relevant to student recruitment and public-facing roles • Information already in the public domain • UoL policies	• University staff directory and staff and student intranets • Teaching material in VLE • Software and Library E resources (licence restrictions) • Strategy & Planning documents pre-publication	• Personal and special category data • Business systems e.g. CoreHR and Banner • Exam papers and assessment material (before assessment) • Disciplinary/grievance proceedings • Information about security vulnerabilities • Legally privileged advice and personnel confidentiality clauses • Draft Strategy documents before approval
Labelling	No specific labelling	✓ Where possible use UoL or Internal in header	✓ Where possible use Confidential in header
Ownership	• All University information (in systems, documents or hardcopy) should have an Owner who is accountable and responsible for the **function** which creates and uses the information. This is Head of Department, Principal Investigator, or Team Leader • Owner must ensure colleagues protect information in line with its classification (i.e. the risks), legislation and University policy		
Protection principle	No access restrictions	Access appropriate to role Protect with min. one barrier (locks/password)	Restricted to role **and** Data Owner authorisation Protect with one or more barriers

Step 2: Store according to classification

	Public Information intended for sharing in the public domain	**Internal** (Default – most information is internal) Information used for day-to-day University functions (accessible to most staff or students); not for general public	**Confidential** Any quantity of Personal data (living people) or info with contractual, business or research value Limit access to least number of people necessary
Physical security	Publicly available and open access spaces within University buildings	1. Use ID card to gain access 2. Sign in and escort visitors 3. Lock screen when away from desk, lock mobile devices and information in cupboards when not in use. Locked file and desk cabinets may be available via Mail and Transport Services Ext. 42557 4. Beware 'shoulder surfers'/'eavesdroppers' to work conversations in public areas	5. Embed clear desk culture and key management for confidential information when not in use 6. Additional locks /door access readers can be purchased via FRCS Service Hub on Ext.43000. 7. Request Campus Support Services to assess the risk and advise on practical safety measures 8. Data Owner to regularly review ID card access 9. Report physical security concerns to Campus Support Services on 0151 794 **3252**
Desktop Computing equipment	• Up-to-date operating system and antivirus is more resilient to malware • Where possible use University issued Managed Windows Service PCs and mobile devices • Do not store/save University passwords on a shared device	1. Use University Managed Windows Service (MWS) PCs, laptops, mobile devices; should be asset tagged and in inventory 2. Keep University password(s) secure; DO NOT share with anyone 3. Protect mobile devices with PIN/Password **and** University encryption software 4. Obtain Head of Department approval **and** appropriate security for overseas travel	5. Use University centrally managed IT facilities[1] to store information, not C Drive of PC/laptop 6. Data Owner is accountable for risk management if using personally owned IT equipment to store Confidential information 7. Risk management controls include: operating system & antivirus updates; hardware encryption; security configuration; access controls and backup and data loss reporting

[1] University of Liverpool centrally managed IT facilities are supported by CSD as System Owner, subject to physical and technical security controls and documentation

	Public Information intended for sharing in the public domain	**Internal** (Default – most information is internal) Information used for day-to-day University functions (accessible to most staff or students); not for general public	**Confidential** Any quantity of Personal data (living people) or info with contractual, business or research value Limit access to least number of people necessary
Business Systems		1. Use University centrally managed IT facilities subject to contract, technical security measures and back up	2. Data Owner to regularly review appropriate access controls, especially joiners, movers and leavers processes
M Drive / OneDrive for Business (work related content and files **not** for shared Team files)	M Drive (UoL data centre) and OneDrive (University Office 365 cloud) only issued to UoL IT account holders, i.e. staff or students with username and password Office 365 login via office.com	1. For work related content and files (M Drive & OneDrive unique to User) 2. User can share personal work files on an ad-hoc basis, BUT user is responsible for managing and maintaining record of shares 3. Access and manage M Drive via VPN, or Apps Anywhere. One Drive login via office.com	4. Users remain responsible for applying and **maintaining** the access permissions to any shared files in their M Drive or OneDrive. 5. **Use centrally managed and supported IT facilities. Manage the risks to the information: take appropriate measures including check and manage permissions; check what and how information is shared.**
University collaboration space: Departmental drives; Active Data Store (RDM) University O365 apps (SharePoint, Teams)	Shared work storage with UoL IT account holders https://www.liverpool.ac.uk/csd/working-from-home/	1. Request Active Data Store (RDM) via ServiceNow Portal (Liverpool Research) 2. Data Owner (Department Head, Principal Investigator, Supervisor or Team Leader) is responsible for managing access permissions to collaboration spaces such as drives ,folders, SharePoint &Teams sites 3. Do not use **free/personal cloud** storage e.g. Dropbox, WeTransfer, icloud, personal OneDrive as not subject to UoL contract, technical assurance or Policy	4. **Use centrally managed and supported IT facilities; including O365 SharePoint and Teams apps. Site owners and users are responsible for managing the risks by checking site, folder and group permissions, confirming who else has access. Limit unnecessary access and manage sharing rights** 5. Principal Investigator/Supervisor should be aware of and comply with the ethics approval and research funder stipulations re. storage

Step 3: Protect the information throughout its lifecycle. Handle according to its classification

	Public Information intended for sharing in the public domain	**Internal** (Default) Information used for day-to-day University functions (accessible to most staff or students); not for general public	**Confidential** Any quantity of personal data, (living people) or info with contractual, business or research value Limit access to least number of people necessary
Share, extract or external transfer (Email/file transfer etc)	Publically available internet pages	1. Think and check (for business reason and approval) before sharing 2. Ensure contracts, data sharing or other formal agreements are in place evidencing responsibilities and safeguards 3. Comply with this Guide for storing digitally (use centrally managed IT facilities) 4. Send a link rather than the document using University collaboration tools: • DatAnywhere or Office 365 apps 5. Zip and Encrypt attachments if emailing	6. Confirm data sharing agreements (and authorisation) 7. Protect and store as per this Guide 8. Protect with encryption before sending: • Secure File Transfer Protocol (SFTP) or Zip and Encrypt before sharing • Issue password using separate method e.g. SMS • Where possible share don't send using Office 365 apps e.g. SharePoint, Teams
Post/courier transfer	• No restrictions	**Internally:** clearly labelled transit envelope **Externally:** sealed, clearly addressed envelope with return address	**Internally:** Clearly addressed sealed envelope or hand deliver **Externally:** Double envelope: outer clearly addressed and sealed, inner envelope labelled as confidential; use recorded or tracked delivery
Data loss reporting/data bearing IT equipment	• Report loss or compromise of personal data **immediately** to the Data Protection Officer legal.services@liverpool.ac.uk • Report equipment, technical or business systems incidents to CSD Service Desk immediately for escalation to relevant team Via ServiceNow: servicedesk.liverpool.ac.uk, via email: servicedesk@liverpool.ac.uk via phone: +44 (0)151 794 **4567** • Ensure your Line Manager is aware		

	Public Information intended for sharing in the public domain	**Internal** (Default) Information used for day-to-day University functions (accessible to most staff or students); not for general public	**Confidential** Any quantity of personal data, (living people) or info with contractual, business or research value Limit access to least number of people necessary
Print / Copy	No printing/copying restrictions	Pick up printing, ensure full document is printed, logout from printer, collect papers after meetings	
Retention	1. Check and apply appropriate retention period at beginning of processing as per UoL Records Retention Schedule 2. At end of retention period, ensure that information is disposed of securely (see below)		
Long term retention and Archive	• Consult with UoL Records Manager and Research Data Manager for physical storage • Follow University Policy and Research Funders policy for long-term archive (as per project's Data Management Plan) • Ensure regular/annual review to confirm retention and identify assets for secure disposal		
Handover (leaving or end of Project)	**BEFORE** leaving/moving role or research project, agree the handover arrangements with Line Manager/Supervisor: 1. Store in UoL centrally managed IT facilities, not user's email (Leavers IT access is disabled and contents deleted in line with Policy) 2. Set up Out of Office message on the Leaver's email account giving an alternative point of contact 3. Ensure Data Owner responsibilities are delegated to another appropriate staff member 4. Remove access rights to confidential material e.g. group email accounts, shared drives/SharePoint, privileged access, ID cards		
Secure Disposal	Public Papers can be recycled – no restrictions on disposal	**Information must be "destroyed beyond ability to recover it", including:** Cross-cut shred or use UoL confidential waste consoles provided by Records Management for paper records. Contact Records management for advice on disposal of USB's, CD's etc Dispose of all data-bearing IT equipment via CSD (for secure erasure and disposal) - this meets environmental waste, recycling regulations and information security requirements Check and delete any temporary store of UoL information on personally owned devices	

This Information Protection Guide supports the University of Liverpool Information Security Policy.