Information Protection Guide V2.0

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. This Guide underpins the University of Liverpool Information Security Policy. At the University, we use the following classifications:

Public	**Internal** (default)	**Confidential**
Information intended for sharing in the public domain	Information used for day-to-day University functions, not for general public	Any quantity of personal data (info about living people) or information with contractual, business or research value
Impact if breached:	**Impact if breached:**	**Impact if breached:**
No adverse impact	Some adverse impact and disruption to services; possible breach of confidence or statutory duty	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 the extra Confidential protection measures.

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 Microsoft365 Confidential sensitivity label
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 (passwords & Duo)	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 papers away when not in use to deter casual theft. Locked file and desk cabinets may be available via Mail and Transport Services Ext. 42557 4. Beware 'shoulder surfers'/ 'eavesdroppers'. 5. Do not use public wi-fi. Use hotspot on mobile phone.	6. Embed clear desk culture and key management to secure confidential info when not in use 7. Additional locks /door access readers can be purchased via FRCS Service Hub on Ext.43000. 8. Request Campus Support Services to assess the risk and advise on practical safety measures 9. Data Owner to regularly review ID card access 10. Report physical security concerns to Campus Support Services on 0151 7943252
Desktop Computing equipment	• Use University Managed Windows Services (MWS) devices • Up-to-date operating system and antivirus is more resilient to malware • DO NOT share University passwords	1. Procure and use University managed (MWS) devices: asset tagged; encrypted; centrally managed Operating System; antimalware protection. See IT AUP 2. MWS is certified for Cyber Essentials 3. Keep University password(s) secure and protect with UoL 2 Factor authentication.	5. Use University MWS and centrally managed IT facilities[1] to store information, not C Drive of device 6. Ensure locally procured storage or device has sufficient security measures as per Infrastructure Management CoP including: authentication, and

[1] University of Liverpool IT Services centrally managed IT facilities and services - 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
		4. Obtain Head of Department approval **and** appropriate IT security for overseas travel	user access controls, encryption; OS updates; antimalware protection and back ups 7. Data Owner is accountable for risk mitigation if using unmanaged devices for Confidential data, as out of scope of Cyber Essentials certification
Business Systems		1. Use University centrally managed IT facilities: subject to contract, assessment, technical security measures and back up 2. Procurement of new IT systems to follow IT Services assessment and prioritisation 3. All systems to use central authentication (Single Sign On) & 2 Factor authentication	4. Data Owner to regularly review appropriate access controls, especially joiners, movers and leavers processes 5. Ensure new systems successfully pass security assessment, solution and service design **before** implementation and use
M Drive & University OneDrive (work related personal files **not** general collaboration)	M Drive (University filestore) and OneDrive (University Office 365 cloud) issued to UoL IT users (staff or students) Office 365 login via office.com	1. For work related content and files (M Drive & OneDrive unique to User) 2. User is responsible for managing and maintaining permissions 3. Manage M Drive shares via VPN, or Apps Anywhere. One Drive login via Office.com	4. Users remain responsible for applying and **maintaining** access permissions to any shared files in their M Drive or OneDrive. 5. **Use centrally managed and supported IT facilities. Check and manage permissions; check what and how information is shared.**

	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
University collaboration space: • Dept. drives; • Active Data Store (RDM) • University O365 apps	Shared work storage for UoL IT account holders See IT Services working from home **Do not use** free/personal cloud storage e.g. WeTransfer, icloud, personal OneDrive	1. Request Active Data Store (Research Data Management) for Liverpool research via Library RDM pages 2. See research data storage options summary 3. Data Owner (Department Head, Principal Investigator, Supervisor or Team Leader) is responsible for access permissions to collaboration spaces such as drives, folders, SharePoint & Teams 4. **Do not use free/personal cloud storage e.g. WeTransfer, icloud, personal OneDrive**	5. Use centrally managed IT facilities, including O365 SharePoint and Teams. Data owner is responsible for access permissions and managing access for joiners, movers and leavers 6. **Share links to documents not attachments. Apply confidential sensitivity label (draft KB)** 7. Principal Investigator/ Supervisor to comply with ethics approval, research funder and contract terms re. research data storage and transfer

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)	Publicly 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 an attachment 5. Zip and Encrypt attachments or encrypt word document if emailing	6. Confirm data sharing agreements (and authorisation) 7. Protect and store as per this Guide 8. Protect with encryption before sending: • Apply Confidential sensitivity label using O365 • Share link to Confidential file using UoL O365 • Otherwise to protect a file as an attachment, before sending, use: ○ Secure File Transfer Protocol (SFTP) or Zip and Encrypt or Encrypt Word document ○ Issue password using separate method e.g. SMS, phone, or teams chat
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

	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
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 IT Services self-service portal immediately https://servicedesk.liverpool.ac.uk via email: servicedesk@liverpool.ac.uk via phone: +44 (0)151 79**4 4567** • Ensure your Line Manager is aware and involved in discussing mitigating actions		
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 University 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 Information & Records Manager and Research Data Manager for physical archive and storage • Follow University Policy and Research Funders policy for long-term archive (as per project Data Management Plan - DMP) • 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		

	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
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 securely following the IT Services approved IT asset disposal process. This ensures secure erasure and disposal and meets environmental waste, recycling regulations and information security requirements. Check and delete any temporary store of UoL information on personally owned devices	

Related Documentation

The Information Protection Guide underpins the University Information Security Policy located at https://www.liverpool.ac.uk/it/regulations/ and includes a number of references and hyperlinks to IT services, research data management and data protection guidance. This Guide will be subject to annual review to ensure that advice and hyperlinks are checked and updated.

Document Control

Document Version Control (published version)			
Author	**Summary of Changes**	**Version**	**Authorised & Date**
Information Security Officer (C Price)	Updates to reflect IT infrastructure changes, sensitivity labelling and general updates	V2.0	IGC: 20/03/2024 IT SMT: 11/03/2024
Information Security Officer (C Price)	Initial Issue. Guidance supporting implementation of the Information Security Policy	Information Protection Guide V1.0 (20200317)	IT Services SMT: November 2019
Document Ownership & Review			
Owner and contact for Enquiries	Information Security Officer, C Price		
Review due	March 2025		
Document location	Regulations, policies & guidelines - University of Liverpool		
**** Owner and Author are responsible for communicating this document ****			