Information Security Policy

Version 4.1

Effective from 01/11/2021

Contents

1.0 Purpose

The purpose of this document is to specify the University of Liverpool priorities for the implementation of Information Security across the Institution.

Information is essential for the day-to-day operations of a University: research; teaching; knowledge exchange; administrative functions; partnership and community work. The University relies heavily on digital technology to collaborate and store information as well as on printed documents and records. Failure to adequately protect and secure information (whatever its form) increases the risk of financial and reputational losses from which it could be difficult for the University to recover.

Information security is the framework of controls around policy, physical security, technical security, training and organisational culture that help to protect the information that is valuable to the University.

This Policy is based on the following standards, regulation and legislation:

- General Data Protection Regulation (GDPR) and ICO Guidance
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- ISO/IEC 27001 & 2
- NCSC Board Toolkit and Cyber Essentials Scheme

2.0 Scope

This policy applies to all people who handle information on behalf of the University as part of their work or role (students, researchers, staff, honorary members and third parties carrying out a University function).

In particular, this policy relates to securing information and working to ensure an appropriate balance of its confidentiality, integrity and availability. Sensitive information that is valuable to the University (whether owned, generated by or entrusted to the University) should be protected from theft, misuse, or compromise that could impact:

- an individual's reasonable expectations of privacy and security;
- the University's ability to carry out its work;
- the University's reputation;
- the University's ability to meet legal, ethical and regulatory requirements.

Information can be written, electronic or verbal and can include: email correspondence; published documents; teaching material; draft plans and strategy documents; exam papers and assessments; data, analysis and findings (both research and institutional data); student and staff information systems; disciplinary or grievance proceedings. Whatever the form, valuable and sensitive information should be protected throughout its lifecycle (collecting, storing, using, sharing, retaining and disposing).

This policy supports and should be read in conjunction with the Data Protection Policy, Records Retention Schedule, IT Acceptable Use Policy and the Information Protection Guide (see Related Documentation Section for links).

3.0 Policy Statements

3.1 Information Security Responsibilities

Information security is effective when using layers of security across physical, technical, policy and personnel security. A single control, individual or department cannot be solely responsible for protecting the University and its information: All members of the University should apply a combination of controls, to maintain and protect the confidentiality, integrity and availability of University information.

A. Users

All members of the University are directly responsible for protecting University (and our partner's) information in accordance with this policy. This includes:

- complying with relevant legislative, regulatory and contractual requirements
- applying protection measures to information in line with its sensitivity and value: i.e. its classification, at all stages throughout the information lifecycle (see Section 3: Information Protection).

B. Business Owners

All information should have a clearly defined owner or custodian. The Business Owner is the senior person responsible and accountable for the function that creates and uses that information (e.g. Dean, Head of Department, Principal Investigator, Research / Academic Supervisor, Manager etc.).

The Business Owner should be aware and maintain a record of the information they are responsible for, including (but not limited to):

- the data types and classification (Section 3) of the information;
- the purposes, use and sharing of the information;
- how access is managed, granted and removed, and training appropriate to role;
- information risk management if storing classified information external to the University centrally managed IT facilities (i.e. ensure baseline technical security measures are met to comply with relevant legislative, regulatory and contractual requirements);
- end of use archive or secure disposal.

C. System Owner/ Administrator

System Owner / Administrator is the role in charge of and responsible for managing the systems which provide the service. This responsibility includes implementing baseline technical security measures including (but not limited to):

- asset inventory / server registration
- physically securing the hardware infrastructure

- patching and updating operating systems
- secure configuration and network connectivity
- full disk encryption on laptops used to store or process University information (default for MWS laptops bought via IT Services)
- user access controls and password security
- back up and availability requirements
- real-time anti- malware protection.

The technical security measures implemented by System Owners should be documented within operating procedures and standards to establish a baseline of controls and to evidence compliance against security frameworks. When the System Owner meets their responsibilities, it will help to ensure the University achieves an appropriate balance of confidentiality, integrity and availability.

i. System Owner/Administrator for centrally managed IT facilities

The IT Services Department (IT Services) is the System Owner for University centrally managed storage, systems, services and infrastructure ("centrally managed IT facilities") that underpin University information assets. IT Services will work in collaboration with the Data Owner to align the Data Owner's business needs for existing and new information systems with centrally managed IT facilities, ensure they are appropriately supported and fulfil the technical security baseline.

IT Services evidence compliance of the centrally managed IT facilities against external accreditation standards, self-assessments, audits and frameworks as a condition of connectivity and to support research requests to receive partner data. These include (but are not limited to): NCSC Cyber Essentials, NHS Data Security & Protection Toolkit and Payment Card Industry Data Security Standard PCI DSS.

ii. System Owner/Administrator for local IT facilities

Where University departments establish local information systems which are outside the remit of centrally managed IT facilities, the Business Owner and System Owner should ensure technical security baseline controls, acceptance of risk responsibility and appropriate documentation are in place that meet the Business and System Owner responsibilities of this Information Security policy.

D. Information Security Officer

The Information Security Officer is responsible for developing and communicating information security policy and associated roadmap that supports a co-ordinated approach across University departments to improve technical, physical, policy and people security measures. This includes providing advice and guidance in collaboration with University information governance practitioners on new systems, information handling, policy implementation and supporting compliance reporting for security frameworks and accreditation.

E. Cyber Security Incident Response Team

The CSIRT is a cross functional team of IT Services staff, with support from Legal & Governance staff, who respond to IT security incidents and policy breaches, associated IT Investigation requests, activity and vulnerability reporting.

A core function of the CSIRT is to effectively investigate the cause(s) of an IT security incident and implement measures to recover and mitigate risk to the University. It is important to learn from security incidents to continue to protect the University, improve awareness and reduce recurrence.

The CSIRT may pass information relating to an IT security incident or breach to external organisations for information or further action. These may include (but are not limited to) the Information Commissioner's Office (ICO), the Police or other Statutory bodies.

F. Information Governance Committee

The remit of the Information Governance Committee (which reports to Formal Senior Leadership Team and for high risk issues to Audit Committee) helps to set direction and be accountable for information governance strategy across the University. This includes monitoring compliance with Information Governance related policies and oversight of information risk management.

3.2 Information Security Values

A. Use centrally managed IT facilities:

University information (owned by or shared with the University) should be stored within University centrally managed storage, systems, services, infrastructure and IT equipment ("centrally managed IT facilities") which are resilient, secure and subject to University approved contract. Centrally managed IT facilities include (but are not limited to):

- University business systems supported by IT Services
- IT Services supported systems and servers within the University on premise data centres
- MWS devices bought via IT Services (with full disk encryption)
- MWS Department/Shared drives, M drive, Active Data Store (RDM)
- IT Services supported cloud services, including University Office 365and central authentications services for Software as a Service providers.

Where research or teaching requirements cannot be fulfilled by using centrally managed IT facilities and local information storage or IT facilities are justified, the Business Owner and System Owner should ensure technical security controls, acceptance of risk responsibility and documentation are in place that meet the Business and System Owner responsibilities (Section 3.1) of this Information Security policy.

B. Accountability:

When developing new strategy, implementing new information systems or local processes, Business Owners within departments should document risk assessment and mitigation to the confidentiality, integrity and availability of their information. Each department should include relevant information risks within their local risk registers.

This Information Security Policy aims to support Business Owners and System Owners to carry out appropriate information risk assessment with relevant templates, checklists and guidance including (but not limited to):

- Data Protection Impact Assessments (DPIA): to assess and include information governance considerations (GDPR, retention, information security and information management) into the early design and planning of new information systems and processing;
- Supplier Security Questionnaire: to assess supplier security accreditations, and data protection compliance prior to procurement
- Risk assessment and acceptance of responsibility if storing information external to the University centrally managed IT facilities;
- Server Management Code of Practice (see Related Documentation)
- Alignment with IT Services Project Management Office and enterprise architecture principles;
- Compliance checklists to support information handling processes in high risk areas (i.e. those handling large quantities of sensitive information).

C. Incident Reporting:

All members of the University who access, use or manage University information are responsible for reporting data loss and security incidents.

Report loss or compromise of personal data **immediately** to the University Data Protection Officer legal@liverpool.ac.uk (in line with the Data Protection Policy) Ensure your Line Manager is also aware.

Report equipment loss, technical or business systems incidents to IT Service Desk immediately. Via portal: https://servicedesk.liverpool.ac.uk via email: servicedesk@liverpool.ac.uk via phone: +44 (0)151 79**4 4567**. Incidents are assessed and escalated to the appropriate team(s) to respond, investigate, and mitigate the risks to the University and its information.

D. Information Handover:

All University information should be returned to the University when its members leave or move to another role (i.e. staff, researchers, honorary members and third parties carrying out a University function). This includes informing appropriate staff of information handover arrangements to ensure the University retains ownership and custody of the information.

E. End of Use:

All members of the University should follow University guidance (University Retention Schedule) for end of use secure disposal or preservation of information. See Information Retention & Secure Disposal section below.

3.3 Information Protection and Classification

The table below summarises the three data classifications which underpin this Information Security Policy. The higher the risk of compromise to information, the more layers of protection are necessary to secure it. Layers will be a combination of physical, technical or procedural security (known as defence in depth) throughout the information's lifecycle i.e. when collecting, storing, using, extracting, sharing / transferring, retaining or disposing of data. Classifying information focuses effort and resources into protecting the most sensitive and valuable information. The Information Protection Guide includes practical guidance on deciding the classification and applying appropriate protection measures.

Public	Internal	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 (about living people) or information with contractual, business or research value
Impact if breached: No adverse impact	**Impact if breached:** Some adverse impact and disruption to services. Possible breach of confidence or statutory duty	**Impact if breached:** Serious privacy or reputational risk, financial impact, commercial disadvantage or disruption to services Breach of statutory / regulatory duty / risk of fine
Information categorised as PUBLIC does not need any special handling requirements.	Access should be appropriate to role and is protected by min. one barrier e.g. username and password for technical security. ID access control or locked office / cupboard for physical security. **Use centrally managed IT facilities (approved cloud and University premises)**	Access to CONFIDENTIAL information should be: appropriate to role **and** authorised by the Business Owner; protected with more than one barrier; encrypted when in transit; shared only with appropriate personnel; securely destroyed at end of use. **Use centrally managed IT facilities (on University premises and approved Cloud) incl. full disk encryption on all mobile storage devices**

There may be limited circumstances where the Business 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 the Information Protection Guide. The Business Owner is responsible for documenting and managing the information risks and safeguards (see Business Owner Responsibilities at 3.1 b) to comply with relevant legislative, regulatory and contractual requirements. For example to comply with Government (HMG) Policy.

3.4 Training and Awareness

The University is committed to supporting and promoting staff awareness of their information security responsibilities to ensure members of the University can understand the risks and apply appropriate protection to the information they handle as part of their role. This is achieved through a framework of policies, guidance, webpages, team briefings and staff obligatory e-learning.

User training will be appropriate to role and identified business needs i.e. staff and postgraduate researchers with privileged access or business areas who regularly handle high risk information may need additional and specific training material or documented operating procedures. Where the Business Owner identifies specific information risks, they should organise additional training that helps to mitigate those information risks. This should be discussed with the Information Security Officer.

3.5 Acceptable Use

The University will have, subsidiary to this Information Security Policy, and the IT Acceptable Use Policy (See Related Documentation) which outlines expected behaviours and activities that all University members (students, researchers, staff, honorary members and third parties carrying out a University function) must comply with. It includes rules for acceptable and prohibited use of University IT facilities and links to relevant misconduct or disciplinary policies in the event of misuse.

3.6 Information Retention and Secure Disposal

University members should be aware of and comply with the University Records Retention Schedule (See Related Documentation section for links). At the end of the retention period information must be securely disposed of to avoid risk of compromise or misuse. Internal or Confidential information should be destroyed beyond the ability to recover it (paying due regard to environmental and legislative requirements around waste and hazardous waste processing). Secure disposal arrangements for data bearing IT equipment and sensitive paper waste will be subject to secure procedures to manage the chain of custody, appropriate contracts and disposal certification from any third party provided secure erasure service.

> **IT Services (Desktop Services team)** is responsible for overseeing the third party provided secure disposal service for data bearing IT equipment. Information remains on IT equipment even when a user has deleted the file, therefore secure erasure and disposal of IT equipment via the IT Services contracted service is mandatory. Donating University computing equipment or removing data storage from computing devices are not secure destruction methods and constitute a breach of University Policy.
>
> https://www.liverpool.ac.uk/csd/my-computer/disposal/

IT Services (Records Management team) is responsible for providing appropriate facilities to support staff to carry out secure disposal of sensitive paper waste via secure locked consoles or confidential waste bags (which are shredded by a third party contractor). Contact Records Management for advice on disposal of USBs and CDs. https://www.liverpool.ac.uk/csd/records-management/storage-and-disposal/confidential-waste/

4.0 Policy Compliance

Failure to comply with this Policy and the Information Protection Guide in protecting University information (or that entrusted to us by a third party) puts the University at risk of reputational damage, financial penalty, breach of legal, contractual or regulatory requirement. It may also lead to disciplinary action in accordance with the relevant Disciplinary Policy (staff or student) or misconduct investigation in accordance with relevant Misconduct Policy.

5.0 Related Documentation

This section lists directly relevant guidance and policies that have been referenced within this Information Security Policy. This policy is subject to bi-annual review which includes a check that hyperlinks within the document are active and up to date. Please contact the IT Services Service Desk to report any broken links, or to raise specific queries.

- Data Protection Policy
- GDPR & Research notice
- DPIA template (Intranet pages
- IT Acceptable Use Policy
- Server Management Code of Practice
- Information Protection Guide
- Obligatory Training: GDPR & Information Security E-learning (Canvas VLE)
- IT Services Information security webpages

6.0 Policy Document Control

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Information Security Officer (C.Price)	Minor revisions to reflect department name changes and related documentation	V4.1	IGC: 15/10/2021
Information Security Officer (Christa Price)	Major revision of policy including revised data classification. Policy replaces: • Information Security Policy V3.0 • Information Asset Classification Policy V1.2 • Workspace & IT Equipment Policy V1.0 • Information Security Review Policy V1.2	V4.0	IGC: 14/10/2019 Formal Senior Leadership Team: 04/11/2019 Council: 20/11/2019
John Cartwright, Chris Woof, Steve Aldridge, Sue Byrne	Subject to reviews Sep 2015, 2016 and 2017. No major changes	V3.0	Council: 28/11/2011
Policy Management & Responsibilities			
Owner	This policy is owned by the Director of the IT Services Department on behalf of the Information Governance Committee. The Director of IT Services has the authority to issue and communicate policy on IT facilities including information security priorities. The Director of IT Services has delegated responsibility for the day to day management, implementation and communication of the policy to the Information Security Officer and will be supported by IT Services teams.		
Policy Review			
Review due:	Biannually by November 2023		
Document Location:	ITS webpages https://www.liverpool.ac.uk/csd/regulations/ University Policy Repository		
** The Owner & Author are responsible for publicising this policy document.**			