Information Security Policy

Version 5.0

Effective from 15/05/2023

Contents

1.0 Purpose

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.

Information is essential for the day-to-day operation and functions of the University: research; teaching; knowledge exchange; administrative functions; partnership and community work. The University relies heavily on digital technology as well as on printed documents and records. Failure to adequately protect and secure information (whatever its form) could lead to serious data loss and compromise, cyber-incident, financial and reputational impact from which recovery could be difficult.

The University will implement information security controls and practices to safeguard its information, while also enabling staff, students, visitors, and partners to access and use the information they need.

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

- UK General Data Protection Regulation (UK GDPR) and ICO Guidance
- Data Protection Act 2018
- Investigatory Powers (Interception by Businesses etc, for Monitoring & Record Keeping Purposes) Regulations 2018
- ISO/IEC 27001 & 2
- NCSC Cyber Essentials Scheme and Board Toolkit

2.0 Scope

Any individual who handles information on behalf of the University as part of their work or role (staff: including researchers and honorary members, students, and third parties carrying out a university function) must adhere to this Policy.

This policy relates to securing university information and working to ensure an appropriate balance of the confidentiality, integrity, availability and safety of the information and systems. 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, security, and safety.
- 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 (but is not limited to): email correspondence; published documents; teaching material; plans and strategy documents; exam papers and assessments; data, analysis, and findings (both research and institutional data); information held on student and staff systems; disciplinary or grievance proceedings. Whatever the form, valuable and sensitive information must be appropriately protected throughout its lifecycle (collecting, storing, using, sharing, retaining and disposal).

This policy supports and should be read in conjunction with (sits alongside) 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: Information Security Framework

An information security framework is effective when using layers of security across physical, policy and personnel, data, technical, and Incident management. It is not sufficient to solely rely on IT Services or previous legacy set up, if initiating new systems, or changing how information is used and processed: each User is responsible for assessing compliance with University Policy requesting support and implementing appropriate safeguards. All users of university information must apply a combination of controls, to maintain and protect the confidentiality, integrity, availability, and safety of university information.

Four simple principles apply:

1. Know what you have
2. Assess the risks
3. Protect
4. Govern and Review

3.1 Know what you have

Requires clear ownership of and responsibility for assets.

A. Accountable Owners: Business / Data Owners

All information must have a clearly defined owner or custodian – called a Business or Data Owner. The Business Owner is usually the senior person responsible and accountable for the function that creates and uses that information from creation to consumption and end of use (e.g., Dean, Head of Department, Principal Investigator, Research / Academic Supervisor, Manager, etc.). The Data Owner may be at any level in the organisation – a small team or even a sole researcher, with responsibility for protecting the information they have been entrusted with.

For consistency of scope, the term Data Owner will be used in this policy.

Data Owners are responsible for ensuring their data is securely managed regardless of location i.e., whether in local departmental systems, in IT Services centrally managed facilities and services or third party hosted solutions: the Data Owner is responsible for putting rules and processes in place around access, use, quality and accuracy, storage and security, and ensuring compliance with those documented rules. Data ownership also applies to each individual user who stores and processes university information and is responsible for protecting it.

B. Asset Registers

Data Owners must know what data, infrastructure, IT equipment, information and IT systems, software, cloud services, and storage they use.

Data Owners (or their delegates), whether at a business area, school, department, or faculty level must maintain and update an Asset Register (See Knowledge Article

Information Security). For IT Services, it is critical to be notified of new devices and systems before they are introduced into the organisation, to ensure end user devices are appropriately protected and managed (See IT Services> Computer Security), and to support an effective cyber security response with the Data / System Owner. IT Services maintain an asset register of centrally managed applications, systems, and services as recorded in the IT Service catalogue.

C. System Owner/ Administrator

System Owners / Administrators are nominated roles: in charge of and responsible for managing the systems which provide the service. This role is sometimes also referred to as Data Steward.

i. Centrally managed IT facilities

The IT Services Department (IT Services) is the System Owner for the University's centrally managed IT facilities, storage, systems, services, and infrastructure ("IT facilities and services") that underpin University information assets. IT Services staff, as System owners for named systems, will work in collaboration with the Data Owner to align and prioritise their requirements for existing and new information systems with the ongoing management of existing IT facilities and services.

ii. System Owner/ Administrator for non-centrally managed IT facilities

If University departments establish local information systems which are not centrally managed, the Data Owner, and their nominated System Owners must manage these facilities to the same minimum-security baseline standards as IT Services. See Section 3.3 Protect

D. Users and Acceptable Use

The University IT Acceptable Use Policy (AUP) (See Related Documentation) outlines expected behaviours that all Users of IT facilities and services (staff, students, researchers, honorary members, and third parties carrying out a university function) must comply with. The AUP includes rules for the acceptable and prohibited use of University IT facilities and services, including responsibility for protecting University information. It links to relevant misconduct and/or disciplinary policies in the event of misuse.

E. Training and Awareness

The University is committed to supporting and promoting staff awareness of their information security responsibilities through a framework of policies, guidance, webpages, team briefings and staff obligatory e-learning.

Training should be appropriate to role. For example, users with privileged access to administer systems, or business areas who regularly handle high risk information, should undertake bespoke training, and adhere to documented operating procedures. Data Owners, as part of their Faculty and Department structure and responsibilities for protecting university information, are responsible for organising

the relevant training within their business area to protect university information and infrastructure.

3.2 Assess the risks

When planning or developing new information systems, IT facilities and services, or new use of information, Data and System Owners should give as much advance notice as possible to relevant central professional services departments (including IT Services, Legal and Finance). This is to:

- ensure effective use of university resources (financial, infrastructure and workforce).
- prioritise workload against existing demands.
- ensure the system meets technical security baselines and enterprise architecture design principles
- assess the impact, and integration with current university systems.
- assess and build in data protection privacy and transparency requirements.

This Information Security Policy supports Data Owners and System Owners to carry out an appropriate assessment by signposting relevant processes and templates. See Knowledge Article Information Security for an overview of key information risk assessment processes.

Where baseline requirements cannot be met, an exception to the policy should be raised. Although this exception will be recorded by IT Services, it should ultimately be assessed, managed, and owned by the Data Owner and/or the System Owner

Data Classification: Assessing and classifying information using the Data classification Scheme (Figure 1 below) focuses effort and resources into identifying and protecting the most sensitive and valuable information. Figure 1 below summarises the three data classifications which underpin this Information Security Policy.

Public	Internal	Confidential
Information intended for sharing in the public domain	Information used for day-to-day University functions not for general public Default classification	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	Access should be appropriate to role and is	Access should be: appropriate to role **and** authorised by the Data/ Business

Public	Internal	Confidential
PUBLIC does not need any special handling requirements.	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)**	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 and services (on university premises and approved Cloud) incl. full disk encryption on all mobile storage devices**

The higher the risk of compromise to information, the more layers of protection (physical, technical, personnel and procedural security) are necessary to secure it. The Information Protection Guide outlines how the University expects different aspects of data classification and protection measures to be applied (from creation through to disposition) by all Users of university information.

3.3 Protect

IT Services provide and are responsible for ensuring centrally managed IT facilities and services meet external security standards, self-assessments, audits, and other regulatory frameworks. Faculty, School and Department Business and System Owners are responsible for adhering to the same standards for any locally procured or legacy systems.

The standards are a pre-requisite for organisations to collaborate on research, obtain funding or to obtain and use partner organisation's data. The standards and certifications include (but are not limited to): NCSC Cyber Essentials, NHS Data Security & Protection Toolkit and Payment Card Industry Data Security Standard PCI DSS, Cyber Security audit.

A. Minimum-security baseline

The minimum-security baseline is a requirement across University IT facilities and services, to comply with information and cyber security requirements as well as external security certifications. A programme of work is underway within IT Services to mitigate risks within centrally managed legacy systems to meet the minimum-security baseline or update to compliant solutions.

Proposals to buy new or to upgrade existing IT facilities and services must be submitted to IT services for assessment, approval, and signoff. The role of IT Services is to confirm that the Supplier, Data & System Owner, and the proposed solution can meet the minimum-security baseline, as outlined below. The Supplier Security Questionnaire (SSQ) Knowledge Article Information Security is the mechanism to assess the minimum-security baseline

Minimum security baseline control	Description
Firewalls and perimeter controls	Ensure only secure and necessary network services can be accessed from the internet, subject to discussion with IT Services.
Secure configuration of equipment including end user devices	Ensure that computers and network devices are properly configured to reduce vulnerabilities and provide only the services required to fulfil their role. See Computer security - University of Liverpool
Software patching	Ensure that software (including operating systems and application systems) is licensed, supported, has automatic updates enabled, and is updated within a reasonable period of an update being released (14 days for critical or high risk)
Vulnerability management:	The ongoing, regular process of identifying, assessing, reporting on, managing, and remediating cyber vulnerabilities across endpoints, applications, and systems
Anti-malware protection:	Ensure real-time malware protection is installed on all devices. To restrict execution of known malware and untrusted software, from causing damage or accessing data
User Identification and Authentication (user access controls and management)	A process to create and approve user accounts, remove or disable access in a timely manner when no longer required, implement a second layer to validate a user. All University information and systems should use IT services managed authentication. IT Accounts must be protected with IT Services multi factor authentication. See Identity and Access Management (IdAM) standard
Activity logging	Audit trail of user and system actions and events to provide traceability of the use of a service
Encryption at rest and in transit	Helps protect sensitive data from unauthorised access
Backing up	Regularly creating a copy of your information so you will always have a recent version of your information saved, which helps to recover quicker if your data is lost or stolen.

Resilience and availability	Information and services should be consistently and readily accessible for authorised parties, and work as expected. All new and existing services should be assessed to ensure appropriate resilience and availability has been specified and built into the system and/ or support model. This should be incorporated within the wider remit of Business Continuity plans and testing for each Business Area.
IT Services Security teams will assess the completed Supplier Security Questionnaire to validate Supplier's evidence that they meet the baseline security requirements to host, to access or to integrate with university data. This is a formal stage within the IT Services Project Management Office processes.	

The Infrastructure Management Code of Practice (see Related Documentation) provides detail on the minimum-security baseline for Infrastructure, servers and shared devices hosted within University of Liverpool environment. Business and System Owners will be expected to evidence responsibilities in clear action plans / security operating procedures. IT Services will also issue guidance on a Shared Responsibility Matrix against minimum security baseline (for on premise and third-party hosted IT facilities and services).

B. Information Handover and End of Use

All University information should be returned to the University when users leave or move to another role (i.e., staff, researchers, students, 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.

All members of the University should comply with the University Retention Schedule for end of use secure disposal or preservation of information. Internal and 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 are subject to contracts and documented procedures to: manage the chain of custody; securely erase or destroy the data; and provide destruction certification from the third party services.

- **IT Services** has a contract with a third-party IT Asset Disposal Partner for secure disposal of all 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. It is each Department's and School's responsibility to ensure all data bearing IT equipment and end user devices are

collected and securely erased by the contracted IT Asset Disposal Partner. https://www.liverpool.ac.uk/it/my-computer/disposal/

- **IT Services (Information & Records Management team)** provide appropriate facilities enabling staff to carry out secure disposal of sensitive paper waste via secure locked consoles or confidential waste bags (which are collected and shredded by a third-party contractor). Contact Information & Records Management for advice on disposal of non-paper confidential waste e.g., USBs and CDs. https://www.liverpool.ac.uk/it/records-management/storage-and-disposal/confidential-waste/

C. Incident Reporting:

All Users of University information, IT facilities and services are responsible for reporting data loss and security incidents.

- Report a loss or compromise of personal data **immediately** to the University Data Protection Officer via Email: legal@liverpool.ac.uk . See https://staff.liverpool.ac.uk/tools-and-services/report-an-incident-or-accident/ Ensure your Line Manager is also aware.
- Contact IT Services Service Desk immediately https://www.liverpool.ac.uk/it/getting-help/.via Phone: +44 (0)151 79**4 4567**.

D. Cyber Security Incident Response Team (CSIRT):

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.

3.4 Govern and review

A security governance framework is not just policy compliance. It is about embedding responsibility for information across all aspects of university work. Enabling the culture that recognises the value and importance of data, how it underpins our business goals, and how it supports all aspects of university research, teaching and learning, professional services, and wider collaboration.

This Information Security Policy is part of the foundations supporting the university to control, direct and communicate cyber security risk management activities.

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 related policies and management arrangements to ensure they are compatible with the strategic direction of the organisation in handling and protecting information throughout its lifecycle. This includes monitoring compliance with Information Governance related policies and oversight of information risk management.

Business Continuity

The University Business Continuity Policy is overseen by the Facilities, Residential and Campus Support Department, with contributions from all relevant areas of the University. All Schools and Departments should maintain, review, and test their local IT Business Continuity Plans (BCPs) to integrate with the University approach.

Payment Card Data Security

The University has an established PCI steering group which oversees the teams managing all payment card processing (and cardholder information) across the University. The Payment Card Industry Data Security Standard (PCI DSS) Finance Policy sets out the requirements for protecting the security of all credit and debit card payments received and processed by the University.

Operating Procedures and documentation

Senior Management Teams in Departments and Schools should oversee and validate that procedures are being documented; for example, as Standard Operating Procedures (SOPs), implemented, and comply with University Policy. The Data/ Business and System Owners are accountable for the information their teams use and must evidence the responsibilities, risk management, technical security controls, and governance measures as outlined in this Information Security Policy.

3.0 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.

4.0 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.

Policies and standards

- Data Protection Policy
- IT Acceptable Use Policy
- Information Protection Guide
- Information and Records Management Policy
- Business Continuity Policy
- Payment Card Industry Data Security Standard Policy
- Server/Infrastructure Management Code of Practice
- Identity & Access Management (IdAM) standard

Supporting guidance and procedures

- Data Protection Impact Assessment (Intranet pages)
- Information Governance Committee Terms of Reference
- Obligatory Training: GDPR & Information Security E-learning (Canvas VLE)
- Service Now Knowledge articles: search for ‘Information security’
- Retention Schedule (for University users)
- IT Services webpages

5.0 Policy Document Control

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Information Security Officer (C. Price)	Major revision to reflect IT Services digital strategy and priorities to meet assurance requirements	V5.0	IGC: Chairs Approval (KR): 09/05/2023 ITS SMT: 05/05/2023 ITS Architecture Board-Endorsed: 03/05/2023
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 university-wide policy on IT facilities and services, including information security priorities. The Director of IT Services has delegated responsibility for the day-to-day development, 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 June 2025		
Document Location:	ITS webpages https://www.liverpool.ac.uk/it/regulations/ University Policy Repository https://www.liverpool.ac.uk/policy-centre/		
** The Owner & Author are responsible for publicising this policy document.**			