LIVERPOOL JOHN MOORES UNIVERSITY

Information Security Policy

Document Author(s):	Registrar and Deputy Chief Executive
Relevant to:	All LJMU Staff
Approved by:	SMT, September 2018
Responsibility for Policy:	Registrar and Deputy Chief Executive
Responsibility for Document Review:	Registrar and Deputy Chief Executive
Date introduced:	April 2013
Date(s) modified:	September 2015, December 2016, August 2018
Next Review Date:	August 2020

RELEVANT DOCUMENTS

- Data Protection Act 2018
- General Data Protection Regulation 2018
- Regulation of Investigatory Powers Act 2000.
- Computer Misuse Act 1990.
- Copyright, Design and Patents Act 1988.
- Copyright (Computer Programs) Regulations 1992.
- The Terrorism Act 2000
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Obscene Publications Act 1994.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Official Secrets Acts 1911-1989.
- The Anti-Terrorism, Crime and Security Act 2001.

RELATED POLICIES & DOCUMENTS

- Staff Handbook
- Code of Conduct for Staff
- Disciplinary Procedure
- Financial Regulations
- LJMU Data Protection Act 1998 Policy
- Records retention policy
- LJMU Freedom of Information Act 2000 Policy and Procedure for Handling Requests
- Conditions of Use of the IT Facilities at Liverpool John Moores University (incorporating the JANET Acceptable Use policy)
- Data Protection Guidance: Microsoft Office 365

Information Security Policy

1. Introduction

Information is a vital asset to any organisation, and this is especially so in a University which is a knowledge-driven organisation, where information relates to learning and teaching, research, intellectual property arising from research, consultancy, administration and management. This policy is concerned with information held by the University and used by members of the University in their official capacities, for example as staff or students. It relates to both computer-based and paper-based information. This policy defines the responsibilities of individuals with respect to information use and to the provision and use of information processing systems.

This Information Security policy can be summarised as the preservation of confidentiality, integrity and availability which is informed by the principles set out in IS0 27001.

All members of the University are directly responsible and liable for the information they handle. Failure to comply with this policy, and other associated policies, may result in disciplinary action.

2. Principles

Appropriate information security involves understanding what information exists, permitting access to all who have a legitimate need and ensuring the proper and appropriate handling of information. The University has adopted the following principles, which underpin this policy:

- Information will be protected in line with relevant laws and University policies, particularly those relating to data protection and freedom of information.
- Information should be available to all who have a legitimate need for it.
- Information must be classified according to an appropriate level of availability: public, open (within the University), confidential, strictly confidential or secret.
- Integrity of information must be maintained; information must be accurate, complete, timely and consistent with other information.
- All members of the University who have access to information have a responsibility to handle it appropriately, according to its classification.
- Clearly identified University staff are responsible for ensuring that appropriate procedures and systems for the processing and holding of information are in place and are effective.
- Information will be protected against unauthorised access.
- Service Level Definitions will be produced, tested and maintained, to ensure that vital information services are available within defined service levels.
- Compliance with this policy is compulsory for all staff and students making use of University information. Breaches of information security controls must be reported to, and will be investigated by, the Data Protection Officer.

3. Definitions

Information

Information takes many forms. For the purposes of this policy, it includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on removable devices. Much of this policy relates specifically to electronic information but the same principles and level of care should be applied to paper-based information. Information may be either structured according to some defined format, or unstructured.

Access

Access refers to any mechanisms by which individuals gain access to information. This policy defines legitimate access and prescribes action to be taken to deal with unauthorised access.

Security

Security refers to mechanisms and procedures designed to ensure that appropriate controls on information access are in place and are effective.

Confidentiality

Confidentiality requires protection of information from unauthorised disclosure or intelligible interception (see below).

Integrity

Integrity involves safeguarding the accuracy, completeness and consistency of both information and computer software.

Availability

Availability involves ensuring information and the associated services needed to process that information are available to staff and students when required.

Computer Software

Computer software is the collection of computer programs used to process information.

Intelligible interception

Intelligible interception is interception of information in such a way that it is readable. Encryption of data may be used to prevent intelligible interception.

Information assets

Information assets include information (see above definition), computer software and hardware.

Username

A unique identifier which is allocated to a member of the University and which, together with a password, is used to identify and authenticate access to a system.

4. Legal obligations and University policies

This policy should be read in conjunction with contracts of employment, University policies relating to the usage of information and systems, and relevant legislation. Relevant University policies include:

- Policy on data protection
- Policy on freedom of information.
- Conditions of Use of the IT Facilities at Liverpool John Moores University (incorporating the JANET Acceptable Use policy).
- Records Management policy.

Relevant legislation includes:

- Data Protection Act 2018
- General Data Protection Regulation 2016.
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Computer Misuse Act 1990.
- Copyright, Design and Patents Act 1988.
- Copyright (Computer Programs) Regulations 1992.
- The Terrorism Act 2000.
- The Anti-Terrorism, Crime and Security Act 2001.
- Official Secrets Acts 1911-1989.
- Obscene Publications Act 1994.
- PREVENT Legislation for Higher Education (prevention of radicalism, violent and non-violent extremism and terrorism).

5. Roles and Responsibilities

All members of the University have direct responsibilities for information, as summarised below. One person often has more than one role. In order to fulfil these responsibilities, members of the University must:

- be aware of this policy and comply with it;
- understand which information they have a right of access to;
- know the information for which they are owners;
- know the information systems and computer hardware for which they are responsible.

Information Users

All members of the University will be users of information. This carries with it a responsibility to abide by this policy and related policies and legislation. No individual should be able to access information to which they do not have a legitimate access right. Systems must be in place to provide controls, but not withstanding this, no individual should knowingly contravene this policy, nor allow others to do so.

Information users must be aware of the nature of the information to which they have access and must handle information appropriately in accordance with its classification. Information users must protect the confidentiality of information and must not deliberately or inadvertently give access to others who do not have legitimate access. Examples of inadvertent access could include leaving confidential printed material where others might see it or leaving data visible on a computer screen where others might view it.

Information Owners

Many members of the University will have responsibility for the confidentiality, integrity and availability of information, for example:

- PVCs, Deans, Directors of Schools, Academic Units and Services are responsible for the confidentiality, integrity and availability of information maintained by members of their department, such as students' academic records. They are also responsible for the security of all departmentally operated information systems.
- Local administrators, IT support staff and other staff in departments may have delegated authority from the relevant Director.
- Data and systems managers in support services are responsible for the confidentiality, integrity and availability of corporate information, such as student, personnel and financial data.
- Project Managers (or equivalent), leading projects for the development or modification of information systems, are responsible for ensuring that projects take account of the needs of information access and security and that appropriate and effective control mechanisms are instituted, so that the confidentiality, integrity and availability of information is guaranteed.

Systems administrators

Computer systems administrators are responsible for ensuring that computer systems are effectively managed, to ensure information confidentiality, integrity and availability. This includes ensuring proper user administration (access controls, security mechanisms) and data administration (access controls, security mechanisms, backup, safe disposal etc).

Information Technology Services staff

The Director of IT Services has overall responsibility for ensuring the technical delivery of policy objectives with respect to the University and for provision of advice, guidance and where appropriate, direction to senior colleagues and departmental IT Support Staff.

Staff in Information Technology Services are responsible for ensuring that provision and operation of University IT infrastructure is consistent with the demands of this policy.

Information Security Officer

The Information Security Officer (Assistant Director of Information Technology Services) is responsible for compliance, investigating actual, potential or suspected breaches of this policy, typically from a technical perspective. In addition, the Information Security Officer provides support and advice to University departments.

Faculty Information Security Manager

The Faculty Information Security Managers (a designated individual within each faculty) are responsible for the implementation of this policy within their respective faculties. For the purposes of this policy, Professional Services is treated as a faculty.

Data Controller
The Data Controller bears legal responsibility for ensuring that the University meets its legal responsibilities for information security. In accordance with the Data Protection Act 2018 and General Data Protection Regulation, the University is the designated data controller. Day to day responsibility for data protection is delegated to the University's Data Protection Officer.

University Records Manager
Many information assets need to be retained for a defined length of time, whether on electronic systems or through other media. This can be dictated by law, regulations, good practice or for organisationally defined business reasons. The University's Records Manager can provide advice on developing appropriate retention policies.

6. Access to information

All information will be classified as described below. Individuals will have access to information according to their role and the data classification. Information owners will be responsible for ensuring that all information is appropriately classified, against defined standards, and for ensuring the review and maintenance of information classification. The University's 'Registrar and Deputy Chief Executive' will be the final arbiter on issues relating to information classification and access.

It is recognized that occasionally an individual may access information unintentionally; in such cases, all members of the University must ensure that they abide by the guidelines appropriate to the classification of the information. Such accesses should be reported in accordance with the classification of the information. Failure to report such access may result in University disciplinary procedures being invoked.

7. Information classification

All information in the University will be classified by those responsible for the information into one of the following categories. Any disagreement as to classification will be resolved in the first instance by a faculty information security officer (or their Professional Services equivalent).

Much information will fall into the *Public* or *Open* categories, but for good reason, such as personal privacy or protection of University interests, some information will be categorised as *Confidential or Strictly Confidential*.

Information may also be categorised as either current, up to date and accurate, or historic, but held for good reason as a record. Historic information may be archived (i.e. retained but removed from prime information sources and possibly stored in a pared down form). Information must be destroyed when there is no valid reason for retention. Disposal must be considered when the information is first acquired.

Public
May be viewed by anyone, anywhere in the world.

Open
Access is available to all members of the University who have a legitimate right to access University IT systems via a username (see section 3).

Confidential
Access is only available to specified members of the University, with appropriate authorisation.

Strictly Confidential
Access is controlled and restricted to a small number of named individuals.

Secret
Known only to a very small number of authenticated LJMU members. Access is subject to, or obtained under, the Official Secrets Act.

Retention Schedule
This policy covers all records, regardless of form or medium, which are created, received and/or maintained by the university, its officers and employees in the course of the University's business. Records created, received and/or maintained in these circumstances become University property and subject to the University policy for the retention and disposal of records. The University must retain certain records for operational and administrative purposes and to demonstrate compliance with statutory or regulatory requirements. There are also various legal and operational reasons why information should not be kept for longer than necessary.

8. Compliance

The compliance and enforcement of this policy will be overseen by the ‘Registrar and Deputy Chief Executive’ who may invoke the University’s disciplinary proceedings when deemed necessary.

The Director and Assistant Director of Information Technology Services will advise the ‘Registrar and Deputy Chief Executive’ and relevant senior staff on matters relating to compliance. Faculty Managers will be responsible for cascading this advice to their academic colleagues. Attention is drawn to laws and policies previously listed in section 4. Users should only access and use information for which they have appropriate authorisation and which is classified as being available to them. Usage of information must be in an appropriate manner. Usage of systems and software must be in accordance with associated policies, laws and licensing constraints, and specific attention should be paid to copyright laws and licence agreements. In certain circumstances, the University will investigate the usage of information and information processing systems.

9. Risk Assessment and Management

Risks assessment and management is seen as a vital component of Information Security. To determine the appropriate level of security measures to be applied to information systems, it is important that a process of risk assessment is carried out for each system to identify the probability and impact of security failures.

10. Incident Handling

Any member of the University must report any information security incident to their local Information Security Manager.

Incidents will be investigated by the local Information Security Manager who will report to the Assistant Director of Information Technology Services. Where appropriate, the 'Registrar and Deputy Chief Executive' will recommend whether there is a potential disciplinary case to answer. The Director of Information Technology Services will, on advice from the Information Security Officer, ensure that appropriate technical steps are taken to address any technical security weaknesses.

11. Implementation

Procedures exist, and are regularly reviewed, to ensure effective information access and security control. The objective of these technical procedures is to ensure that:

- Information users are appropriately identified and have access to information for which they have a legitimate need
- Computer systems are appropriately managed and controlled in line with the requirements of this policy
- Information assets are identified and protected
- There is clear assignment of responsibilities

The procedures include:

- User registration procedures, authentication mechanisms and password usage for access to all computing facilities
- Control of, and mechanisms for, access to University computer networks, network system security, intrusion detection, prevention and remedial action
- Systems security mechanisms, including monitoring and logging, automated security patching and virus protection
- Backup of computer systems
- Inventory of equipment assets
- Systems change control, testing and acceptance for corporate information systems.
- Information access control for different classifications of information, database administration, regular review of user access rights
- Management of privileged systems access
- Disaster recovery and business continuity, aligned with the Business Continuity Plan

- Physical security of computer rooms and network hubs
- Computer maintenance and regulated disposal of redundant equipment

12. Storage of University Computer-based Information

Introduction

All University Computer-based Information Assets must be stored on server systems provided by Information Technology Services unless prior written approval has been granted by the Registrar and Deputy Chief Executive or the Director of Information Technology Services. It is strongly recommended that all University Computer-based Information Assets are stored on server systems operated by Information Technology Services. Critical information assets are held on resilient storage devices. They are backed up on a regular basis to devices located in secure environments. It is recognised that for some very large data sets it may be impractical to store this on Information Technology Services operated systems. However, Information Technology Services must still be consulted about the storage and management of such data.

Where University Computer-based Information Assets are not stored on servers provided by Information Technology Services, then steps must be taken to ensure that appropriate data backup procedures are in place and operational. Where information assets are stored on devices external to LJMU, contracts managed by Information Technology Services must be in place to ensure: emergency access to the information is available to the Director of Information Technology Services or a designated deputy when deemed necessary, and that the storage of information assets complies with relevant legislation.

Core Systems

For data held within the University's core systems (e.g., Finance System, Student Information System, CRM, Staff InfoBase, Aleph, Blackboard) the user need take no specific action; these systems automatically store the information in databases that are held on IT Services managed servers and storage devices.

Email System

All University business conducted by email must be held on University provided systems and email accounts to ensure the security and confidentiality of University business and to ensure the University can comply with a person's right to access any records it holds.

Data held within the University's email system is secure and backed up on a regular basis. University Computer-based Information Assets should not be stored only within the email system: the primary copy of any such Information Asset should be stored in a centrally managed storage location e.g., M: drive, OneDrive for Business[1], SharePoint.

Managed Clients

Computer-based Information Assets (including Word documents, spreadsheets and Access databases etc.) that originate on Information Technology Services

[1] See Appendix B for more information about OneDrive for Business.

Managed Client PCs or similar systems should be stored on a centrally managed storage device.

All registered computer users are provided with both a network drive (M:) and One Drive for business which are accessible whenever the user is logged on to a managed client. For individuals that do not use Managed Clients, other ways are provided for using this disk space e.g., Off Campus Applications, Office365 portal and OneDrive for Business Apps. Users should therefore store University Information Assets on the facilities provided and not on the local hard disk drive of their machine. Access to both the M: drive and OneDrive for Business is secure and it requires the username and password of the owner to access the file space. By default, no other user has access to the data. In exceptional circumstances, access may be granted to specific files or folders, with the express permission of the Director of Information Technology Services or a designated deputy.

Use of Local Storage Devices

University computer-based Information Assets must not be held on the hard drives of PCs or other systems in offices, laboratories etc. as these are not normally secure against theft, damage due to fire, flood or vandalism, or other incidents including malware infection (*see Compromised Systems below*). A centrally managed storage device (e.g. M: drive and OneDrive for Business) or an approved alternative should be used instead.

University Information Assets must not be stored on personal systems that are located on non-University premises, e.g. a user's home PC.

Use of Laptops and Mobile Devices

Users of mobile devices need to be particularly vigilant and take appropriate steps to ensure the physical security of the device at all times, but particularly when travelling or working away from the University. Access to all devices must always be controlled by the use of proper usernames and passwords, or a PIN, as appropriate.

Compromised Systems

When a PC[2] becomes infected with a virus or other malware, or is compromised in any way, the data on that PC and any data storage that it accesses is at risk. When an infection/compromise of any kind is suspected or confirmed, the affected PC must not be used until it has been confirmed as 'clean' by IT Services. In most cases, this will require that the PC be rebuilt before it can be used again.

[2] This includes fixed 'desktop' PCs and mobile devices such as laptops or tablets.

Appendix A Data Classification

The LJMU Information Security Policy defines the high level Information Classification categories which will be applied to all LJMU data and information. (see LJMU Information Security Policy Section 7).

This Appendix expands this high level classification to provide more detailed descriptions of the kinds of data and information which would be covered within the agreed categories.

Restricted data:

Restricted data relates to all data that is not categorised as “Public” in the Information Access Matrix: even data classified as “Open” has a degree of restriction in that it is only available to authenticated LJMU members.

Different types of data fit within different security levels, each of which has a level of risk attached should this data be lost, leaked or misused. The Matrix shows the University data and risk classifications, with examples of data that fit into each classification.

Further information about the Freedom of Information Act can be found on the Secretariat webpage at http://www2.ljmu.ac.uk/secretariat/

Control:

It is recommended that given that sensitivity of specific data items may be determined by a range of functions across LJMU, an overview of the operation of the Data Classification Policy is managed by the Records Management function within the University Secretariat.

Information Access Matrix

	RESTRICTED DATA				
	Public	**Open**	**Confidential**	**Strictly Confidential**	**Secret**
Risk	None	Low	Medium	High	Critical
Definition	May be viewed by anyone, anywhere in the world	Access is available to all members of the University who have a legitimate right to access University IT systems via a username.	Access is only available to specified members of the University with appropriate authorisation.	Access is controlled and restricted to a small number of named individuals.	Known only to a very small number of authenticated LJMU members. Access is subject to, or obtained under, the Official Secrets Act.
Examples	1.Term and closed dates. 2.Staff names, job titles and work contact details. 3.Faculty names, codes and addresses. 4.School/Programme, unit and	1.Student names and email addresses. 2.Staff webpages. 3.Available staff categories. 4.Normal calendar entries. 5.Assessment details (i.e. assessment types, titles, etc.)	1.Staff/student addresses and personal details. 2.Next of kin details. 3.Staff/student photographs. 4.Student admission/registration details.	1.Staff salary and grades unless stipulated under the Freedom of Information Act (further details from the Data Protection Officer at link on top of page).	1.Anything subject to or obtained under the Official Secrets Act. 2.Some Freedom of Information requests exempted under national security (See link above).

	department/division names. 5.HESA subject and fee status codes. 6.Anything subject to disclosure under the Freedom of Information Act (see link at top of page). 7.Staff publications.	6.Library Catalogue. 7.Blackboard learning materials. 8.Sharepoint document repositories.	5. Individual student exam timetables. 6. Individual student assessment information	2.Staff/student medical history. 3.Staff/student racial or ethnic origin including other categories listed in the Equality Act 2010 (See link at top of page) 4.Exam candidate numbers. 5.Personal information as defined by the GDPR. 6. Procurement information defined as commercial-in-confidence and or covered by a non-disclosure agreement (NDA) 7. Staff/student passwords, authentication verifiers, private keys.	

For any personal data you need to process or otherwise use, refer to the Personal Information Access Matrix in the first instance and assume, as a rule of thumb, that anything not covered defaults to strictly confidential.

Personal Information Access Matrix

		Classification					
Data subject	**Information attribute**	**Public**	**Open**	**Confidential**	**Strictly Confidential**	**Secret**	**Notes**
Staff member	Name	x					
	Date of birth				x		
	National Insurance Number				x		
	Equality/Diversity information				x		
	E-mail address	x					
	Telephone	x					
	Common username		x				
	Photograph			x			1
	Home Address			x			
	Salary				x		
	Bank details				x		
	Medical information				x		
	Publication	x					3
	Password				x		
Student member	Name		x				2
	Date of birth				x		
	National Insurance number				x		
	Equality/Diversity information				x		
	E-mail address		x				2
	Common username		x				
	Photograph			x			
	Home Address			x			
	Medical information				x		
	Programme		x				
	Units		x				

	Department		x				
	Student number			x			
	Bank details				x		
	Password				x		
	Assessment Component		x				
	Classification of Final Award			x			
	Final Assessment Item		x				
	Final Award and Title			x			
	Finalised Module Mark			x			
	Mark for Assessment Component			x			
	Overall Award Mark			x			

This matrix defines levels of *read access* to various categories of electronic information.
Any information attribute that is not listed here defaults to 'Strictly Confidential' in classification.
Any member of the University may request that exceptions to this scheme are made for them; any decision rests with the Registrar & Deputy Chief Executive and/or the Data Protection Officer.

Classification:	Public	Visible to anyone
	Open	Visible to any authenticated member of the University
	Confidential	Visible to some authenticated members of the University
	Strictly Confidential	Visible to a small number of authenticated members of the University
	Secret	Known to a very small number of members of the University;

Notes

1 Any staff member can alter the classification of their photograph to 'Open' or 'Public'

2 Any student member can alter the classification of these attributes to 'Public'

3 There are exemptions for some research publications which will not be classed as 'Public' – For further Information contact the Data Protection Officer.

OneDrive for Business

OneDrive for Business is online cloud based file storage available to all LJMU staff and students. This storage allows users to:

- Store up to 1 terabyte of content online
- Upload files up to 2 Gb in size
- Create new or edit existing documents using Microsoft's online Office applications
- Share files with other LJMU Office 365 users

All data deposited in the University's OneDrive for Business service is stored within Microsoft's data centres located in the EU. The University retains full ownership and control over the data and is satisfied that the data is properly secured and protected. OneDrive for Business must be used in compliance with University policies and procedures.

What can and cannot be stored in OneDrive?

The OneDrive for Business service is intended to augment the M: Drive and shared storage options available to staff and students rather than replace specific services.

It should be noted that OneDrive for Business is developed, operated and supported by Microsoft. OneDrive for Business may be used for seamlessly accessing, updating and sharing general use files from multiple locations and devices.

The following table details which classifications of data may (or may not) be stored on OneDrive for Business.

Classification	Definition	Storage
Public	May be viewed by anyone, anywhere in the world.	This information may be stored on OneDrive for Business.
Open	Access is available to all members of the University who have a legitimate right to access University IT systems via a username.	This information may be stored on OneDrive for Business.
Confidential	Access is only available to specified members of the University, with appropriate authorisation.	This information may be stored on OneDrive for Business with the appropriate access controls to ensure only those staff or students that need the information can access the information.

Classification	Definition	Storage
Strictly Confidential	Access is controlled and restricted to a small number of named individuals.	This information **cannot** be stored on OneDrive for Business.
Secret	Known only to a very small number of authenticated LJMU members. Access is subject to, or obtained under, the Official Secrets Act.	This information **cannot** be stored on OneDrive for Business.

It should also be noted that the following types of data or information **cannot** be stored on OneDrive for Business:

- Data that is subject to a specific contractual agreement that specifies a particular storage method (that is not OneDrive for Business).
- Data that is subject to a specific contractual agreement that prohibits storage in a Public Cloud Service.
- Research data where the funding body has stipulated that the data must be physically housed[3] within the University.

[3] Unlike OneDrive for Business, other centrally provisioned storage options such as the M: Drive are physically located within the University's own datacentres.