University of Lancashire

IT Security Policy

Applicable from September 2025 to Present

Title: IT Security Policy					
Version	**Issue Date**	**Revision description**	**Author**	**Approved by & date**	**Next review date**
1	Sept 2019	-	-	Academic Quality and Standards Committee: May 2019	May 2020
2	Sept 2025	Update to University name and move to new template	-	Academic Quality and Standards Committee: May 2025	May 2026

Purpose of policy	The IT Security Policy sets standards outlining the way electronic information and IT systems should be managed and operated to ensure the University complies with its obligations in relation to IT Security. The policy sets out how all users of University IT systems and the information they contain must act to ensure these standards and obligations are met.
Internal services involved in authorship & implementation	Learning and Information Services
Related University regulations, policies & guidance	Network Lite Fair Usage and Security Policy Rules for the use of IT facilities Rules for the use of the Library Learning and Technical Services Loans Policy Wireless Network Fair Usage and Security Policy
Procedure lead	IT Engineering Manager
Equality impact assessment date	Equality Impact Assessment (EIA)
Data protection impact assessment date	Information Governance - Home

Contents

1 INTRODUCTION

The University uses a large amount of information in order to operate effectively and the majority of this information is in electronic format and held on computers its IT systems. It is essential that this information is managed effectively so that it remains secure, accessible to authorised users and its integrity is protected. The IT Security Policy sets standards outlining the way electronic information and IT systems should be managed and operated to ensure the University complies with its obligations in relation to IT Security. The policy sets out how all users of University IT systems and the information they contain must act to ensure these standards and obligations are met.

A glossary of terms is available at the end.

2 SCOPE OF THE POLICY

The IT Security Policy covers all internal and external University systems and connections to wider networks. It sets out how information contained within or accessible via those IT systems should be handled to ensure it remains secure. It must be read in conjunction with the Rules for the use of IT Facilities and Wireless Network Fair Usage and Security Policy which are available on the Student Contract pages of the University website.

All internally and approved externally hosted systems must conform to this policy. The University reserves the right to isolate any IT system including externally hosted service or networks, which represents a potential or actual breach of security; to monitor information sent over its networks; and to deny user access to the universities, approved IT systems.

3 POLICY STATEMENT

The University recognises the importance of keeping its information and IT systems secure and protected from unauthorised use. Through compliance with this policy, the University will ensure that all corporate information generated, used and held electronically in IT systems, networks, media and related forms is accurate, secure and available to authorised users for business purposes when needed.

4 RESPONSIBILITIES

This policy applies to all students, employees, including temporary, casual, contract and agency staff, as well as any contractors, guests in Microsoft Office 365 and service providers acting on behalf of the University.

The Chief Operating Officer (COO) has overall responsibility for ensuring the University complies with this policy. The COO is supported in their responsibility by the Learning and Information Services department (LIS). Any questions or concerns about the operation of this policy should be referred in the first instance to the LIS Customer Support Team LISCustomerSupport@lancashire.ac.uk or Ext. 5355.

This policy is reviewed annually by LIS on behalf of the COO. Recommendations for any amendments should be re

ported to LIS Head of IT Security for consideration as part of the review process. The University will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

5 RELATIONSHIPS TO OTHER POLICIES

This policy must be read in conjunction with the following policies and guidance

applicable to the user:-

- Rules for the use of the University's IT facilities
- Email Use Policy
- General Data Protection Regulations (GDPR) Policy (and associated guidance)
- Freedom of Information Policy
- Rules for the Use of the Library
- Wireless Network Fair Usage and Security policy
- Network Lite Fair Usage and Security policy
- Storing and Sharing Information
- University of Lancashire Information Categories

The following policy applies to all users and can be found virtue link provided:-
Acceptable Use Policy of JANET(Joint Academic Network)
https://community.jisc.ac.uk/library/acceptable-use- policy

6 GENERAL – IT SECURITY POLICY FOR ALL STUDENTS

The information in this section of the policy is applicable to all users of the University's computer systems. All users must read and comply with this section and any other applicable sections.

6.1 PERMITTED USE

All users of IT facilities must adhere to the rules set out in this IT Security Policy. Users are also required to conform to the current Rules for the use of IT Facilities and Wireless Network Fair Usage and Security Policies.

6.2 USER AUTHORISATION

The University will ensure that all computer system users are formally authorised to use the network and keeping a maintained audit trail of authorisation. Students are authorised through the enrolment process as being fee-paying students of the University. Guest access to Microsoft's Office 365 Teams and Groups is authorised and the responsibility of the Microsoft Office 365 Teams or Groups owner.

6.3 USER ACCOUNTS AND PASSWORDS

Individual users will each be given a personal University account for which they are held responsible. The account is for the sole use of the authorised user for access to the University's IT facilities. Users must not permit their account to be used by anyone else. Users must not use or attempt to use someone else's account.

Passwords must be kept secure at all times and not be shared. If a password needs to be written down or stored, it must be in a format that could not be recognised by others.

All users are required to register to use the self-service password service using the registration web page https://passwordregistration.lancashire.ac.uk.

If a user forgets their password, they must create a new one using the Self-Service Password Reset web page https://passwordreset.lancashire.ac.uk

Users can change their own passwords without administrator intervention, either on a University computer using the Change Password application from the Start menu or through the self-service password service.

Users must follow good security practices when selecting passwords. Passwords should be at least eight characters in length and should include numbers, mixed case letters and symbols. They should not be made up of strings of the same characters,

real words or common passwords such as family names, car registration numbers, telephone numbers and days of the week or other aspects of the date. These types of password are easy to crack and can lead to security breaches due to unauthorised access.

If users suspect that their password may be known to an unauthorised party, they should change their password immediately and not use it ever again.

Users should use a different password for their university account than any personal/private accounts.

6.4 ID CARDS AND ACCESS CONTROL CARDS

Lost or misplaced corporate ID cards present a security risk as information they contain may, in some circumstances, allow an unauthorised access to organisational information or other significant parts of computer systems. The loss of cards used for access to buildings or secure rooms can potentially lead to a breach of physical security.

To guard against such events, all lost or stolen cards must be reported to LIS Customer Support (liscustomersupport@lancashire.ac.uk or 01772895355) at the earliest opportunity but no later than 48 hours. Any reported lost card will immediately be disable. Users can obtain a replacement card from the <i> in the library.

Lost cards that are found must be handed in to the security desk in the library. Security will inform the owner that the card has been found. Lost cards will only be returned after proof of identity. To help protect the personal information held on ID cards, the old card be physically destroyed if not claimed.

6.5 SYSTEM ADMINISTRATION

User ID's are not allowed local administrative rights on University computers by default. Sensitive system commands and software are restricted to system administrators and security personnel. Accounts with enhanced file access rights or with high-level access to computer systems will only be used when necessary to perform tasks requiring such access. Excessive and unnecessary use will expose the computer system to increased risk of virus infection and damage to the file system and software.

6.6 KEEPING INFORMATION SECURE

Individuals who use the University's computer systems to process personal data must comply with the requirements of the current Data Protection Legislation as set out in the Data Protection Policy and associated guidance.

For mobile devices such as laptops, tablet computers, smartphones etc; the user must ensure the device PIN or password has been set and that the device is set to automatically lock after a short period of inactivity. This will help protect the device against misuse and is an extra safeguard for any personal contact details or any other confidential information held on the device. However this does not replace the need for encryption. Any device without a PIN or password as a minimum-security measure must not be used to hold any organisational or personal information.

Users should note that if a device is lost or damaged, the information stored on it may not be recoverable. These types of devices should therefore never be used to store the only copy of information.

Where encryption is used, encryption passwords must be kept securely and separately. Encrypted information cannot be accessed without the encryption password.

6.7 PHISHING, VISHING AND SPAM

Information security not only involves technical security measures but also requires users to ensure they act appropriately to maintain the security of computer systems and the corporate network. Attackers aim when attacking these systems and networks is to obtaining organisational information, cause damage or disruption to that information by infecting them. Users should be aware of such attacks and be able to recognise them in order to stop them being successful. Attacks may involve phone calls from individuals trying to obtain confidential information by deception or may occur by email.

Users must ensure that organisational information is only disclosed by phone to callers who are authorised and entitled to receive that information. Further information can be found in the Data Protection Policy.

Users must ensure that they do not click on links in spam or phishing emails or emails which appear to be such. Attachments to such emails must not be opened. Spam and phishing emails are becoming more and more sophisticated and plausible, if in any doubt, do not open the mail and delete it or contact LISCustomerSupport@lancashire.ac.uk on 01772 895355 for advice.

Users must never email their usernames and passwords in response to emails. An increasingly common practice adopted by criminals attempting to gain access to passwords, is by telephoning and posing as a member of IT Support Staff. LIS Customer Support will never ask for your password. If you receive such a call **DO NOT** give your password, hang up and report it to LIS Customer Support on 01772 895355, who will arrange for an IT Security investigation.

If users are in any doubt, they should contact LIS via LISCustomerSupport@lancashire.ac.uk or 01772 895355 for advice.

6.8 BACK-UP AND RECOVERY OF INFORMATION

Students are advised to use their allocated Home Area(N:\) for storing of files. Home area drives are backed up daily by LIS systems. For staff, all organisational information must be stored in compliance with the University's Information Categories document.

Users must not store organisational information on individual computers or devices unless exceptional circumstances apply, following advice from LIS and the Information Governance Officer (where personal data is involved). The LIS system administrators cannot and do not back up files held away from the University network.

6.9 CLOUD SERVICES

Users must follow the University's Data Protection Policy when handling data. The only cloud storage service approved for the storage of non-Public categorised information is Microsoft Office 365 Services. This includes but not limited to;

6.10 Microsoft OneDrive for Business
6.11 Microsoft Exchange Online
6.12 Microsoft SharePoint Online
6.13 Microsoft Outlook
6.14 Microsoft Teams and Groups

A full security and compliance risk assessment has been undertaken of Microsoft's Online Services by the University of Lancashire.

Users of this service need to be aware of the following;

6.15 The University has no direct control over the availability of this cloud service

6.16 Responsibility for the availability, backup and recovery of the service lies with Microsoft.

6.17 Deleted files can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost forever.

6.18 Microsoft can and do carryout periodic updates and maintenance, which may result in a loss of service for that period.

It is recommended that important/critical documentation is kept on, or at least backed up to, the user's N: drive (Home area), which is backed up daily.

For further advice, contact LIS customer Support on ext. 5355 or by email at LISCustomerSupport@lancashire.ac.uk

6.19 SOCIAL NETWORKING

Students should not use their UCLan email addresses on their private social media accounts as this may compromise the security and privacy of the University's email system. The exception to this requirement is where accounts are used for interaction in genuine academic circles. For advice and assistance, contact LIS customer Support on extension 5355 or by email at LISCustomerSupport@lancashire.ac.uk

6.20 WORKING FROM HOME/REMOTE WORKING

Users must note that when using home PCs or other equipment at fixed locations outside the University, they are operating outside the University IT security perimeter.

It is the responsibility of users to ensure that PCs used for home working are themselves properly secured. Weak security on home PCs used for home working could lead to the compromise of their account and result in security incidents involving University IT systems.

Users are responsible for the safeguarding of equipment against unauthorised access, misuse, theft, or loss when in their home or in transit. Where home computers are used by other family members, no organisational information should be accessible by such unauthorised parties

Users must ensure that all reasonable protection measures are in place and operating where applicable, as follows:

- The computer's local Firewall should be enabled
- Anti-virus software should be installed and set to automatically update itself
- Anti-spyware software should be installed to provide continuous protection against malicious software being downloaded
- Up to date security patches should be installed for both the operating system and applications when released by software vendors and set to automatically update itself
- Wireless networks at home must be properly secured against eavesdropping and intrusion.

Users must comply with the security requirements of this document at all times and where personal data is being processed, they must also comply with the Data Protection Policy.

Users must not access internal or confidential/sensitive information over unsecured broadband or public wireless networks as these present a security risk. Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

6.21 COPYRIGHT

Copyrighted and licensed software must not be duplicated, removed or added by users unless it is explicitly stated that this is acceptable.

The University's IT systems and network infrastructure, including wireless and Network-Lite must not be used for the downloading or streaming of copyrighted materials including but not limited to video and audio files, without the written consent of the owner or copyright-holder.

6.22 USE OF SOFTWARE

Copyrighted and licensed software must not be copied or distributed by users in contravention of the licensing agreement. Users are not permitted to trial software, for example from a removable disk on University computers, and are not permitted to modify the operating system either manually or by downloading applications such as screensavers, themes etc.

Personal use of peer-to-peer networking and file sharing applications is not permitted on any of the University's systems. These applications use University resources for non-University purposes, they increase the risk of virus infection and spyware, which compromise privacy and security and could involve legal risks regarding the storage of copyrighted material.

7 NETWORK MONITORING

7.1 AUDITING

Computer logs are records of past events and can be used to aid investigations into fault finding, security incidents or misuse of the University's IT systems.

Types of information recorded in computer logs include (but are not limited to):

- The dates and times of account logins and logouts
- Internet use and network traffic
- The behaviour and health of the computer system itself
- Network performance

Use of computer accounts and Internet usage will be logged and recorded in order to comply with the Jisc/Janet contract. Software logs will be enabled as appropriate to comply with license conditions. Where appropriate, computer systems will log user activity to assist in any investigations. Attempts to breach security will be investigated immediately. System administrators regularly review computer logs to detect attempts to breach system security. Where checks of computer logs raise suspicions of attacks on the computer system, actual security breaches or other irregularities, system administrators will promptly investigate such concerns.

7.2 SECURITY BREACHES

Users must report all suspected or actual security breaches as soon as they become aware of it, using either the Incident Reporting Form (staff only) or LIS via LISCustomerSupport@lancashire.ac.uk or 01772 895355. This applies regardless of whether they have caused, or are informed of, a breach. LIS will ensure that any security breaches reported to them are acted upon promptly and will keep appropriate records and documentation. Corrective actions taken and other resolutions will be documented and monitored. In cases where an incident involves personal data, it must be reported to the Information Governance Officer using either the Incident Reporting Form (staff only) or LIS via LISCustomerSupport@lancashire.ac.uk or 01772 895355 without delay. This will then be managed and reported in line with the Information Governance Incident Procedure.

8 GLOSSARY OF TERMS

Glossary	
User	The individual who uses the computer systems
Computer systems	All campus networks, servers, workstations and network access devices
Organisational information	Information relating to the running of the University. This may be personal information about students, staff, external customers and contractors; information shared with the University by its business and research partners; or corporate information which is confidential or commercially sensitive.
Personal data	As defined by the Data Protection Act 2018: Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be an opinion (such as aspects of an employment reference). Information can be personal data without including a person's name. Personal data may also be referred to as 'personal information'.
Security incident/breach/violation	Any incident where the security of the computer system, corporate network or organisational information is compromised e.g. due to unauthorised access or disclosure.
Cloud services	Online storage areas hosted by commercial organisations external to the University where information can be stored and accessed via an individual user account e.g. Google Cloud.
Corporate network	Any and all infrastructure intended to support the corporate IT requirements.
Non-standard hardware and software	Any equipment which does not have an LIS-developed and maintained operating system. This is the case even if the equipment is funded by the University.


1828
University of
Lancashire