University of Lincoln Acceptable Use Policy

AUP Quick Guide

You are expected to be familiar with the full AUP and to behave responsibly when using University Digital Services resources.

Access and Usage

- Use only assigned username and password for University DS resources, following the password policy
- Do not access unauthorised information or use unauthorised DS resources
- Ensure compliance with license agreements and copyright obligations

Content and Internet Usage

- Do not share indecent, obscene, pornographic, or terrorist-related material without written authorisation
- Do not display discriminatory, offensive, illegal, or defamatory content
- Do not send commercial, copyrighted, or unsolicited content using University email resources

Email Usage

- Use University email addresses for university business only
- Do not automatically forward emails from university staff email addresses to non-University addresses
- While limited personal use is allowed, it should not disrupt University business

System Integrity and Security

- Do not engage in behaviour that damages University DS resources or affects other users
- Use DS resources in a way that upholds the University's reputation
- Never introduce harmful software, such as viruses, to any University DS resource
- Staff must register their personal devices with Microsoft Intune to access University services

Data Storage

- Personal data should be stored on University OneDrive or provided shared drives.
- Authorisation should be obtained before storing personal data on portable devices
- Special category data should not be stored on portable devices without authorisation.

University of Lincoln Acceptable Use Policy

Document Control	
Owner:	Tim Ingham, Head of Digital Security and Compliance
Contact:	DS@lincoln.ac.uk
Version number:	3.0
Approval date:	May 2024
Approved by:	Digital Services Delivery Board
Date of next review:	May 2025

1. Purpose

1.1 This document defines the University of Lincoln's Acceptable Use Policy (AUP) for Digital Services (DS) resources.

It is designed to support all areas of the University's business and to recognise academic freedoms when using DS resources. The intention is that this policy will enable the University to carry out its activities by protecting and preserving University DS resources at the appropriate level.

This policy is intended to protect the digital and information assets of the University by adopting the core principles of information security:

- Confidentiality – the prevention of unauthorised disclosure of information
- Integrity – the prevention of corruption or unauthorised amendment or deletion of information
- Availability – the prevention of unauthorised withholding of information or resources

It also ensures that the University meets its statutory duty under the Counter Terrorism and Security Act 2015, termed PREVENT. This duty aims to aid the process of preventing people from being drawn into terrorism.

Throughout this document, the term Sensitive Data refers to any or all of the following:

- Personal data
- Special Category Personal Data
- Confidential data
- Highly Confidential data

Further information on information classification can be found in the University of Lincoln's Information Ownership and Classification Policy.

2. Scope

2.1 Who is covered by this policy?

This policy applies to all users of University of Lincoln resources regardless of their role, including, but not limited to:

- Students enrolled at the University
- Permanent staff employed by the University
- Temporary, casual or agency staff working for, or on behalf of, the University
- Contractors, consultants and suppliers working for, or on behalf of, the University
- Visitors to the University

Users, as defined above, whether on or off campus, submit to be subject to this policy when they:

- Access data or DS resources belonging to the University on any device, whether provided by the University or personally owned or
- Access DS resources on behalf of the University in the course of their official University duties, studies or research (including but not limited to networks, devices, software or cloud services), or
- Use 3rd party resources in connection with their official University duties, studies or research (e.g. blogs, chat, vlogs, social media)

2.2 What DS resources are covered by this policy?

This policy applies to DS resources and systems made available for use by users by, or on behalf of, the University of Lincoln, including but not limited to:

- PCs, including desktop PCs, laptops, Apple Macs or other computers
- Mobile devices, including smartphones, tablets and other smart devices
- Networks with wired, wireless or internet connections
- Internet services
- Email and other messaging, social networking or collaboration services
- Application software, services and data, including databases
- Peripherals e.g printers, copiers and scanners
- Removable media, such as external hard drives, memory sticks and other legacy media such as DVDs
- Access to resources using personal devices, e.g. devices not provided by the University of Lincoln

3. Roles and Responsibilities

3.1 When using DS resources, users are expected to comply with the following:

Access and Usage

1. You must only use your assigned account username and password to access University DS resources; the password must comply with the password policy.
2. You must not access any information you are not permitted to access.
3. You must not use any DS resource you are not permitted to use.
4. You must not use any DS resource contravening any applicable license agreements or copyright obligations.

Content Usage

5. You must not display, store, transmit, or knowingly receive images, text, or any other material that could be considered indecent, obscene, pornographic, or of a terrorist nature unless you have a legitimate reason for doing so and have written authorisation from your academic supervisor or head of department. The University reserves the right to monitor and/or block access to such material.
6. You must not display, store, transmit, or knowingly receive images, text, or any other material that is or could be considered discriminatory, offensive, abusive, racist, or sexist when the context is a personal attack or might be considered harassment.
7. You must not display, store, transmit or knowingly receive images, text or any other material which could be considered illegal, paedophilic or defamatory.
8. You must not send commercial material, software or any copyrighted material belonging to parties outside of the University or belonging to the University itself without legitimate permission from the owner.
9. You must not send unsolicited emails (‘spam’), chain letters or any unauthorised or unsolicited content using University email resources.
10. You must not send unsolicited emails (‘spam’) to a large number of recipients without authorisation from Digital Services.

System Integrity and Security

11. You must not engage in behaviour that damages or adversely affects any University DS resources or the ability of other users to use them.
12. You must not use any DS resource in a way that brings, or may bring, the University into disrepute.
13. You must not knowingly introduce malicious software, such as viruses or similar threats, into any University DS resource or other DS resource.
14. You must not compromise or risk compromising the security, confidentiality, availability, or integrity of the University’s DS resources in any way.

Identity and Authorization

15. Further to 1, you must not use another user’s identity or otherwise disguise your own or their identity when using any DS resource.
16. You must not use a DS resource for any unauthorised purpose.
17. External organisations or users that contract to abide by this policy agree to ensure that their partners and subcontractors also contract to abide by it as a condition of their partners or subcontractors using DS resources covered by this policy.

4. Internet and Email Usage

4.1 The University internet connection is provided by JANET, which connects the UK's education and research organisations to each other and the rest of the world through links to the global Internet. JANET and this policy require that users abide by the prevailing JANET Acceptable Use Policy.

4.2 Internet Usage

In addition to those items covered in the Content Usage of 3, it is unacceptable to use the University Internet connection or University networks to:

- Upload, download, link, embed or otherwise transmit commercial software or any copyrighted materials without permission unless this is covered or permitted under a commercial, licence or other such agreement.
- Download any software, data or other material without implementing effective virus protection measures.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses or sustained high volume network traffic that substantially hinders others in their use of the network.
- Install or use software or applications to monitor network traffic or contents or scan devices connected to the network.
- Upload sensitive data to the Internet or to unapproved cloud-based storage (e.g. Dropbox) without authorisation from your supervisor or line manager AND without ensuring it is strongly encrypted. The University's Office 365/OneDrive is the only approved cloud storage provision for sensitive data.

4.3 Email Usage

When using University email systems for University related business, you are expected to adhere to this policy, as well as all relevant laws and other University policies and regulations.

You must only use University email addresses for University business.

Staff members must not automatically forward emails from University staff email addresses to student email addresses or to non-university/private email addresses. Doing so could compromise security by moving data to an external environment beyond the University's control and contravenes the University's Data Protection Policy.

While reasonable personal use of email is allowed, it should not disrupt University business in terms of volume, frequency, or time expended.

The contents of personal emails are private and will not be investigated or monitored except in limited and exceptional circumstances, as outlined in section 4.4.1. It is recommended that personal emails be stored in a separate folder clearly marked as personal.

Please note that email information is inherently insecure. Email information should be considered insecure or unprotected while in transit unless encrypted using an appropriate method.

The University provides anti-virus and spam filtering services to email users. While efforts are made to keep these services effective and up-to-date, the University cannot guarantee protection against all viruses, phishing campaigns, or spam.

4.4 Internet and Email Monitoring

DS infrastructure is typically monitored to ensure its efficient and effective operation. This routine performance monitoring does not involve accessing or reading the content of shared drives or emails. However, the University keeps backups of information which might subsequently be accessed as part of a properly authorised investigation in accordance with English law.

Statistics and data relating to the use of University DS resources may be made available to third parties, such as the police, in accordance with English law. This may occur when a lawful request for this information is received, when the University is legally obliged to do so, or when it is appropriate for other reasons.

The University also reserves the right to demand that passwords and decryption keys, where used, be made available. This allows the University to fulfil its right of access to material when a lawful request for this information is received or when the University is legally obliged to do so.

4.4.1 Investigations

Authorisation for an investigation or monitoring will be sought after a complaint has been received about suspected violations of this or other University policies or regulations or as part of a wider investigation, including allegations of illegal activity.

Any investigation or monitoring is subject to the following safeguards:

- The Department of People Performance and Culture (PPC) will authorise the investigation or monitoring for staff-related investigations or Student Support and Wellbeing for students.
- Monitoring or investigation will only occur when the authorising senior member of the University Staff is satisfied there are grounds for suspecting criminal activity or serious malpractice.
- The investigation or monitoring will be carried out by technically competent staff with appropriate training.
- Records about what was accessed, when, and by whom will be kept.
- Under normal circumstances, the individual(s) concerned will be notified in advance unless, in the opinion of the authoriser, notification would hinder preventing or detecting wrongdoing.

4.4.2 Access to Email and Personal Storage

For staff accounts, as email and personal storage are primarily provided for business and academic use, it might be necessary to grant another staff member access to an individual user's accounts for important business purposes. This could include accessing time-sensitive information when a user is in long-term absence or otherwise unavailable. Where possible, permission from the mailbox owner should also be sought in the first instance. However, if this is not possible, the mailbox owner's line manager must request it from the DS Service Desk.

5. Use of Staff Personal Devices for University Business

5.1 The University recognises that personal devices play an ever-increasing role in day-to-day business activities. The University is responsible for ensuring the security of its systems and data; thus, all personal devices accessing this data must be registered, secured, and compliant.

5.2 Microsoft Intune is a cloud-based tool that enables the University to manage user access to organisational resources and simplify app and device management across the organisation.

Staff users wishing to use their personal device(s) to access University services or systems must register their device(s) with Microsoft Intune. Depending on the device and the level of access required, there are varying levels of protection. Full details and guidance can be found on the DS support web pages.

6. Data Storage

6.1 Users responsible for processing personal data electronically should store it within the University OneDrive or on University-provided shared drives. Additionally, consideration should be given to using an additional folder, file, or database-level password protection, access restrictions, and/or encryption.

Users intending to store personal data on portable storage devices such as laptops, tablets, memory sticks, hard drives, disks, or mobile phones must obtain authorisation from their supervisor or line manager. Personal data on portable storage devices must be encrypted, and the device must be stored in a lockable filing cabinet, cupboard, or drawer.

Staff members are prohibited from keeping special category data on portable storage devices unless they have received authorisation from their supervisor, line manager and the University Information Compliance Team.

If personal data is processed off-site electronically, it must be done using University-approved equipment and/or systems, including remote access mechanisms such as OneDrive, University Cloud Desktop, or University provided Virtual Private Network (VPN).

7. Payment Card Processing (PCI-DSS)

7.1 Staff and students in 'staff' roles must exclusively use approved PCI-DSS compliant payment collection devices, such as approved tills, PDQ devices, or secure online payment applications on approved computers, to enter or direct others to enter Credit/Debit card numbers and associated security codes.

7.2 Writing down card information on paper, typing it into emails, storing it in spreadsheets, or using non-approved systems/devices is strictly prohibited. If you receive an email containing a Credit or Debit card number, immediate deletion is required to maintain compliance with PCI-DSS requirements.

8. Policy Violations

8.1 Reporting Policy Violations

Violations of this policy can be reported to:

- DS Service Desk on x6500 or dt@lincoln.ac.uk
- abuse@lincoln.ac.uk – particularly for email issues
- ISM@lincoln.ac.uk – the Digital Security Manager

If a violation of this policy involves personal data, then the University Data Protection Policy requires that the Data Security Breach Management Procedures be followed by contacting:

- compliance@lincoln.ac.uk - University Information Compliance team

8.2 Consequences of Policy Violations

Depending upon the circumstance, the consequences of violations of this policy could be any combination of:

1. Access to any or all DS resources covered by this policy being denied.
2. Appropriate disciplinary action under the terms of university regulations or staff contracts of employment.
3. Cancellation of contracts between the University and the user or the organisation that the user works for, or on behalf of.
4. In serious cases, violations of this policy may result in expulsion from the University or termination of a contract of employment.
5. In serious cases of violations of this policy the University or other parties may take civil or criminal action against the user.

9. Disclaimer

The University will not be liable, beyond any statutory liability, for any loss, damage, or inconvenience arising directly or indirectly from the use of or prevention of the use of any DS resource.

The University also accepts no liability, beyond any statutory liability, for any DS material submitted to or processed on any DS resource. Similarly, the University also accepts no liability, beyond any statutory liability, for any DS material deposited at or left on University premises.

10. Agreement for External Parties

This form must be signed by external staff, contractors, or third-party organisations that are to be allowed to use University of Lincoln DS facilities.

I/We (delete as appropriate) agree to abide by this University of Lincoln Acceptable Use Policy:

Date:

Signed for on behalf of an organisation (when applicable):

Full Name:

Company Name:

Signed for by the individual

Signature:

Name:

Position:

Telephone:

Email address: