IT Acceptable Use Policy

Version 3.4

Effective from 06/02/2024

Contents

AUP Quick Guide 2
1.0 Purpose and Scope 3
2.0 Policy Statements 4
2.1 Acceptable IT Use - Users shall: 4
2.2 IT facilities when Users leave 5
2.3 Prohibited IT Activity: Users must comply with the following conditions: 6
2.4 Exceptions 7
3.0 Policy Compliance 7
3.1 Logging and Monitoring of IT Facilities 7
3.2 IT Activity Investigation 8
3.3 Breach of Policy 8
4.0 Related Documentation 9
5.0 Policy Document Control 10

IT Acceptable Use Policy

AUP Quick Guide

You are expected to be familiar with the full AUP and to behave responsibly when using University IT facilities and services.

- IT Identity – You're responsible for all activity on your IT account: keep your IT password secret; don't share your IT credentials with anyone (especially phishing scams); don't attempt to obtain or use anyone else's IT credentials

- IT Protection – Maintain an up-to-date operating system, anti-malware protection, and software updates on your computing device, to protect all University information and systems. Don't introduce malware, unauthorised or unlicensed software, or interfere with hardware or services

- IT Behaviour – Use University information, IT facilities, and services responsibly and with respect for other Users. Don't waste IT resources, don't interfere with others' legitimate use, or behave towards others in a way that isn't acceptable in the physical world

- IT Information – Safeguard personal data, respect other people's information, and don't abuse copyright material. Use University centrally managed IT facilities and services to store University information

- IT Governance – Comply with the IT AUP and observe the regulations of third parties whose facilities and services you access. Don't break the law or damage the University's reputation. All use of University IT facilities and services is logged. Investigation of IT logs is carried out where there is a specific and proportionate need concerning policy breaches, security incidents, or a request from law enforcement

- Report it – Report concerns or ask for IT help via the IT Services self-service portal https://servicedesk.liverpool.ac.uk

1.0 Purpose and Scope

This IT Acceptable Use Policy (AUP) applies to anyone using the University of Liverpool's centrally managed IT facilities and services (whether on or off campus). The AUP outlines acceptable and prohibited use of University IT facilities and services, as well as Policy compliance measures. Any individual accessing University information, IT facilities, or services (whether via personally owned or University issued devices) is deemed to have accepted this Policy. It is expected that members of the University apply the same standards outlined in this AUP to non-University IT. Compliance with the terms is a condition of connection.

'Users' includes (but is not limited to):

- Staff and Students;
- Members of Council and associated committees, contractors, honorary staff, external partners, and associate members carrying out a function on behalf of the University, including (but not limited to): external examiners, committee lay members;
- Students and staff from other institutions logging on using Eduroam;
- University tenants using University IT facilities and services;
- Visitors accessing University online services including guest Wi-Fi.

IT Services is delegated to provide centrally managed IT facilities and services to the University. These include (but are not restricted to):

- On-premises infrastructure and network services, applications, storage, and business systems, including connection to the internet.
- University-approved and contracted cloud services including (but not limited to): Microsoft 365 One Drive, Teams and SharePoint, IT services managed Software as a Service (SaaS) services and applications, video conferencing tools, services procured or accessed through university research funding and/or external grants.
- Software and electronic resources required to effectively carry out the University's business purposes.
- End user devices and data-bearing IT equipment used to access and process University information, including (but not limited to): PCs, laptops, tablets, telephony and mobile phones, servers, portable storage devices, and multi-function printers.

Where users (with line manager approval) have decided to use locally procured or personally owned devices to access University information and/or carry out University business functions (also referred to as Bring Your Own Device - BYOD), such end-user devices and data-bearing IT equipment), **must** be protected with equivalent technical and procedural security measures, as the University centrally managed end-user devices. Please see section 2.1.5 below.

This policy is non-contractual, but all users of the University of Liverpool's IT facilities must comply with this Policy.

This policy may be updated periodically, to comply with requirements of legislation, JANET (UK) Policies, and University Policies. Updates will be communicated as part of the regular policy review and key service announcements to all Users.

It is each User's responsibility to keep up to date with changes and obligations of this Policy.

2.0 Policy Statements

2.1 Acceptable IT Use - Users shall:

2.1.1 Utilise the University IT facilities and services responsibly and respectfully following:

a. UK law, (or relevant overseas law when accessing University IT facilities and services from that country); and
b. University Policy, in particular recognising the Safeguarding Policy outlines rules and responsibilities for under 18's accessing University facilities; and
c. Regulations of any third parties whose facilities and services Users' access.

2.1.2 Recognise that IT facilities and services are provided primarily for university business purposes to support teaching, learning, research & enterprise, and professional & administrative activities.

2.1.3 Understand that occasional and reasonable personal use of the IT facilities and services is acceptable however, University business purposes take priority over personal use of IT facilities. Any personal use of IT facilities and services must comply with University Policy and not interrupt, distract, or deny services to other Users, or otherwise conflict with an individual's obligations to the University.

2.1.4 Be aware of their responsibilities and the impact their behaviour and use of the University's IT facilities and services may have on other users, members of the public, and on the University's reputation. This can include behaviours not related to IT such as fraud, theft, bullying, and harassment. Email and other communications using University IT facilities and services are potentially retrievable and subject to disclosure under Freedom of Information, Data Protection, or other legal proceedings.

2.1.5 Take appropriate measures to protect University information, IT facilities, and services from malware, data breach, misuse, or other compromises. Appropriate measures include:

a. be responsible for all activity using their University IT account. All users must be authenticated to use University IT facilities and services (I.e., usage is attributed to identified users)
b. keep passwords secret, do not share, or disclose your IT account or system passwords. Do not leave computers logged in and unattended
c. use strong passwords at least 12 characters long; do not reuse your university password on other sites and change your password immediately if there is suspicious account activity. See IT Services guidance on passwords and protecting IT accounts
d. do not respond to scams and 'phishing' requests for credentials, or passwords or click on links and attachments in unsolicited or unexpected emails. If unsure stop and check via the IT Services Service Desk
e. ensure computing and storage device(s) connecting to University IT facilities and services have an up-to-date, secure, patched, valid licensed operating system **and**

anti-malware with real-time protection enabled, to connect to the network. See IT Services security guidance

f. Locally procured (non-IT Services) storage devices must be registered with IT Services. Devices should be encrypted where possible. (See Related Documentation for Infrastructure Management Code of Practice)
g. use IT Services centrally managed IT facilities and services (including IT Services issued accounts for University business. Do not use personal accounts. Centrally managed IT facilities and services are subject to contract, support, and minimum security baseline as outlined in the Information Security Policy
h. complete available digital skills, and role-specific and obligatory training modules to use IT facilities appropriately and effectively
i. comply with the licensing and copyright conditions of maintained and supported software, equipment and electronic resources made available as part of the University IT facilities and services. Ensure any locally obtained software applications and systems have a valid license and are patched promptly as updates are available, as required by Cyber Essentials. All software applications and systems must be compatible with and use the University central authentication Single Sign On (SSO) and Multi Factor Authentication (MFA) services as per minimum security baseline (Information Security Policy)
j. take responsibility to check software vendor's terms and license conditions and that you can comply with those terms and conditions, before obtaining or requesting installation. Remove software that is no longer patched or maintained from the end user device.
k. prevent loss or theft of IT equipment accessing University information, particularly personal data or information that is sensitive and/or confidential: encrypt devices storing University personal data, do not leave unattended in public, prevent casual access using a PIN, password, or device lock, protect the device when not in use
l. report security incidents, actual or suspected breaches of this policy, and loss, theft or compromise of IT equipment storing University Information via the IT Services self-service portal: https://servicedesk.liverpool.ac.uk. Report incidents (loss, breach, or compromise) relating to personal data immediately via your line manager and Data Protection Officer

2.2 IT facilities when Users leave

Creation and termination of access to IT facilities and services (including IT accounts) are informed by the start and end dates in the Human Resources and Student Records systems. Access to IT facilities and services is removed after the end date. Before leaving the University, Users must:

- complete information handover to their Line managers / Supervisors and Tutors to ensure University information is appropriately retained within University IT facilities and services;
- return University IT equipment (in reasonable working condition), information, and resources to the University (removing any copies stored locally in non-University systems or devices); and

- ensure any of their data that they wish to keep (but not data that is the property of the University) is removed, as access to University IT facilities is removed after the end date.

2.3 Prohibited IT Activity: Users must comply with the following conditions:

2.3.1 not breach UK law, University Policy, or Regulations of third parties whose facilities or services are accessed as part of university business purposes.

2.3.2 not create, view, download, store, send, transmit, or cause transmission of any material that is abusive, obscene, discriminatory, racist, harassing, threatening, derogatory, defamatory, pornographic, extremist, or otherwise indecent or illegal.

2.3.3 not share your university IT account password.

2.3.4 not deliberately access, obtain, alter, or delete personal data for purposes or uses outside of their job-specific access to said personal data.

2.3.5 not gain unauthorised access (or enable others to gain unauthorised access) to University IT facilities regardless of intent: to make, supply, or obtain anything in order: to commit or facilitate crime; to deny access; to deliberately misuse; to cause unauthorised modification, impairment, harm, or significant damage to the University IT facilities and services or the IT facilities and services of other organisations.

2.3.6 not intentionally or recklessly introduce to the University IT facilities any form of spyware, computer virus or other potentially malicious software, data interception, password detecting or similar monitoring or traffic capture software or devices, that will bypass security controls including (but not limited to) VPN anonymisers or Internet Proxy services, that will disrupt the work of other Users, facilitate the theft of data or IT facilities or impact the correct functioning of the University IT facilities and services.

2.3.7 not connect any hubs, switches, routers or wireless routers to the University network. All such devices must be approved and / or managed by IT Services.

2.3.8 not tamper with networking or IT Services provided equipment, or continue to use systems, hardware, or devices that IT Services have requested cease, have disconnected, or have required appropriate remediation be completed.

2.3.9 not carry out IT activities that will:

a. intentionally or recklessly use the name of the University or any of its members in such a way that either by content or expression brings the University into disrepute

b. incite hatred, radicalise themselves or others (as per the Prevent Duty Section 26(1) of the Counter Terrorism and Security Act 2015)

c. advocate or promote any unlawful act

d. be likely to defame, defraud or deceive another person or organisation

e. cause harm, harassment, bullying, discrimination, victimisation, needless anxiety, or persistent nuisance to others

f. corrupt, destroy, facilitate the theft of data, deny, or disrupt services to other users, such as unnecessary or trivial messages, chain, junk mail, or unsolicited bulk or marketing email (spam)

g. plagiarise or infringe copyright, breach software licence terms, trademark, or Intellectual Property, or infringe the proprietary rights of another person or organisation. This includes using unlicensed or 'cracked' software, downloading copyright protected material without permission or use of streaming services to bypass paid subscriptions

h. conflict with an individual's obligations, contractual or otherwise to the University leading to personal financial gain or competing with the University in business

i. agree to terms, enter into contractual commitments, or make representations by email on behalf of the University, unless authorised and appropriate to do so

j. conflict with the University obligations via the JANET (Joint Academic Network Security Policies) (See Related Documentation section) such as the use of IT facilities for non-University commercial purposes.

2.4 Exceptions

2.4.1 In the event of unexpected absence where information/correspondence is not in shared repositories, or there is incomplete handover when changing or leaving a role/project, the University may need access to communications or information stored in an individual's IT account (email, file storage) to fulfil operational business/statutory purposes. **Operational Access Requests** are subject to assessment and authorisation on a case-by-case basis and must be proportionate to the operational business/statutory purpose. Operational Access Requests are separate and distinct from IT Activity Investigation Requests (section 3.2 below) which relate to handling allegations of inappropriate use of IT facilities.
The Operational Access Request is included in the Information Access catalog in the IT Services self-service portal: https://servicedesk.liverpool.ac.uk.

2.4.2 In the course of properly authorised and supervised University work or research, Users may have a requirement to access material that falls within the criteria of Prohibited IT activity (section 2.3 above). The User and User's Department / Institute must discuss and agree on appropriate risk management procedures including health & safety duty of care, appropriate legal, governance, and secure data management arrangements before completing the Internet Exception Form.
The Internet Exception Form is included in the Information Access catalog in the IT Services self-service portal: https://servicedesk.liverpool.ac.uk.

3.0 Policy Compliance

3.1 Logging and Monitoring of IT Facilities

IT Services logs use of University IT facilities and services. IT Services will monitor IT logs and take appropriate action to protect and promote the confidentiality, integrity, and availability of University IT facilities and services; including using security tooling to identify and investigate technical or security-related problems, supporting security incident response, and providing evidence in the event of misconduct or criminal investigations.

Monitoring is overseen by the IT Services Security Operation Centre (SOC). Monitoring is only carried out to the extent permitted or as required by law, under the Data Protection Act 2018 and the Investigatory Powers (Interception by Businesses, etc. for Monitoring and Record-keeping Purposes) Regulations 2018, as necessary and justifiable for business purposes. These purposes include:

- To monitor the effective function of the IT facilities and services (system maintenance and administration)
- To investigate, detect or prevent the unauthorised use of IT facilities and services
- To monitor whether the use of the IT facilities and services is legitimate and following this policy
- To comply with any legal obligation.

3.2 IT Activity Investigation

Where there is a concern or request to investigate an individual's use of IT facilities and services, an IT Activity Investigation Request Form must be completed. IT activity investigations should only be initiated where there is a specific and justified need concerning an allegation of misuse or policy breach, an IT security incident, or a formal request from the Police or other regulatory or law enforcement body. Monitoring the effective function of the IT facilities i.e., system maintenance and administration, does not fall within the scope of an investigation. IT Activity Investigation Requests should be:

- justified and proportionate to the incident/usage causing concern,
- discussed with and endorsed by the professional service department overseeing the appropriate policy (i.e., staff disciplinary policy, a policy of student conduct and discipline, academic or research misconduct policies)
- appropriately authorised by the Head of Department or another authorised role holder and the Director (or authorised Deputy) of the IT Services Department
- managed following university disciplinary and/or misconduct policies and procedures, and be subject to clear scope, approval, documentation, and evidence handling procedures by the IT Services Cyber Security Incident Response Team (CSIRT) to ensure the findings are admissible in a formal dispute or legal process. This process also ensures that staff members are supported and do not commit an offence by looking for potentially illegal material.

3.3 Breach of Policy

Misuse of IT facilities and services can damage the University and its reputation. Breach of this policy may be dealt with under the University's policies including the staff disciplinary policy, policy of student conduct and discipline, academic or research misconduct policies; and, in serious cases, may be treated as gross misconduct leading to summary dismissal or termination of studies.

In the event of a breach of this Acceptable Use Policy, serious security vulnerability, or security incident the IT Services CSIRT will, on behalf of the University, exercise discretion to:

- Access, restrict, or suspend a User's access to University IT facilities and services.
- Take down content.
- Disconnect or block systems, computing equipment, or end-user devices.
- Manage the IT activity Investigation (involving the examination and disclosure of IT logs) to support those nominated to undertake the relevant Disciplinary or Misconduct Procedure investigation, following the staff disciplinary policy, policy of student conduct and discipline, academic misconduct, or research misconduct policy.
- Refer the information to the police, regulatory body, or other law enforcement agency in connection with a criminal investigation.

4.0 Related Documentation

This section directly lists policies that are relevant when accessing University IT facilities.

- JANET (UK) Connection, Security & Acceptable Use Policies
- Information Security
- Telephony & Call Recording Policy
- Information Management Policy
- Data Protection
- Social media compliance policy
- Policy on the Safeguarding of Children, Young People, and Vulnerable Adults
- Staff-related Policies including Staff Disciplinary
- Research-related Policies including Research Misconduct
- Export Control rules
- Student-related Policies including Student Conduct & Discipline and Academic Integrity

Guidance and Forms

- Operational Access Request, IT activity Investigation Request and Internet Exception forms are part of the Information Access Catalog located within the IT Services self-service portal: https://servicedesk.liverpool.ac.uk >Requests> Information Access forms
- IT Account request forms Online forms - University of Liverpool
- Infrastructure Management Code of Practice and the Shared Responsibility Matrix clearly define responsibilities for securing servers and related infrastructure
- Server and NAS (Network Attached Storage) registration forms are part of the Hardware catalog located within the IT Services self-service portal: https://servicedesk.liverpool.ac.uk >Requests>Hardware>Server Registration
- IT Services webpages: https://www.liverpool.ac.uk/it/

5.0 Policy Document Control

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Information Security Officer (C Price)	Minor updates to reflect security protection measures and updated supporting guidance	V3.4	Information Governance Committee: 31/1/2024
Information Security Officer (C Price)	Minor amends to reference security protection measures	V3.3	Information Governance Committee: 27/01/2023
Information Security Officer (C Price)	Minor amends to the AUP to reference department name change, clearer definitions, and incorporate aspects of Cyber Essentials	V3.2	Information Governance Committee (IGC): 23/06/2022
Information Security Officer (C Price)	Minor amends to the AUP to reference anti-malware protection and BYOD (Bring Your Own Device).	V3.1	Information Governance Committee (IGC): 17/06/2021
Information Security Officer (Christa Price)	Major revision of IT Regulations into IT Acceptable Use Policy (AUP). The AUP replaces: IT Regulations V2.1; Security Investigation Policy V1.2; Information Security Incident Response Policy V1.2	V3.0	Information Governance Committee (IGC): 12/06/2020 FSLT: 22/06/20 Council: 07/07/20
J Cartwright, C Woof, S Aldridge, S Byrne	Subject to reviews Dec 2015, and Aug 2017. No major changes	V2.1	Corporate Services & Facilities Committee: 06/03/2012
Policy Management & Responsibilities			
Owner	This policy is owned by the Director of IT Services (Chief Digital Information Officer-CDIO). The CDIO has the authority to issue and communicate policy on IT facilities and services including information security priorities. The CDIO has delegated responsibility for the day-to-day implementation and communication of the policy to the Information Security Officer and will be supported by IT Services teams.		
Policy Enquiries	Please direct any queries about this Policy to the IT Services self-service portal: https://servicedesk.liverpool.ac.uk		
Policy Review Due: Annually by July 2024			
Document Location:	IT Services webpages https://www.liverpool.ac.uk/it/regulations/ University Policy Centre https://www.liverpool.ac.uk/policy-centre/		
** The Owner & Author are responsible for publicising this policy document. **			