IT Acceptable Use Policy

Version 3.0

Effective from 22/07/2020

Contents

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.

- 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 – Use up to date antivirus software and operating system on your device. Don't damage the University IT facilities by introducing malware, unauthorised software or interfering with hardware or services

- IT Behaviour – Use University IT facilities and systems 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 to store University information

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

- Report IT – Report concerns or ask for IT help via the CSD 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 IT facilities. The AUP outlines acceptable and prohibited use of University IT facilities, as well as Policy compliance measures. Any individual accessing University information and using the University IT facilities (whether on personally owned or University issued devices) is deemed to have accepted this Policy and is bound by the terms and conditions included within.

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

- Staff and students (whether on or off campus);
- 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;
- Visitors accessing University online services including guestnet wifi.

University IT facilities include (but are not restricted to) the following services and equipment provided by the University of Liverpool and third parties on its behalf:

- Network and infrastructure services across University premises providing connection to the internet, wireless, web applications, business systems, Email and University contracted online services such as Office365 and video conferencing tools;
- Data bearing IT equipment (including but not limited to: PCs, laptops, tablets, smart phones, multi-function printers, servers) purchased and managed via the Computing Services Departments (CSD);
- Software and Electronic resources required to effectively carry out the University business purposes;
- All data bearing IT equipment bought or implemented outside of CSD for University business purposes.

This policy is non-contractual but all users of the University of Liverpool's IT facilities have a duty to comply with this Policy.

This policy may be updated periodically, in order to comply with requirements of UK law, JANET (UK) Policies and University Policy. Updates will be communicated as part of the regular policy review

2.0 Policy Statements

2.1 Acceptable IT Use - Users shall:

2.1.1 Utilise the University IT facilities in a responsible and respectful manner in accordance with:

a. UK law, (or relevant overseas law when accessing University IT facilities from that country); and

b. University Policy; and

c. Regulations of any third parties whose facilities Users access.

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

2.1.3 Understand that occasional and reasonable personal use of the IT facilities is acceptable however, University business purposes take priority over personal use of IT facilities. Any personal use of IT facilities 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 IT facilities may have on other users of the facilities, members of the public, and on the University reputation. This can include behaviours not apparently related to IT such as fraud, theft, bullying and harassment. Email and other communications using University IT facilities 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 and IT facilities from malware, data breach, misuse or other compromise. Appropriate measures include:

a. be responsible for all activity using the issued University username and password (all use of IT facilities must be attributed to identified users)

b. keep passwords for accessing University IT facilities secret, do not share your account password or leave computers logged in and unattended

c. use strong passwords at least 8 characters long; do not reuse your University password on other sites and change your password immediately if there is suspicious account activity. See CSD guidance on password and protecting IT accounts

d. do not respond to scams and 'phishing' requests for credentials, passwords or click on links and attachments in unsolicited or unexpected emails

e. ensure computing device(s) connecting to the University IT facilities have up to date, patched, valid and licensed operating system **and** anti-virus protection. See CSD security guidance

f. use University issued accounts and IT facilities for University business rather than using personal accounts. Centrally managed IT facilities and storage are subject to contract, support and baseline technical security measures as outlined in the Information Security Policy

g. complete available digital skills, role specific and obligatory training modules to use IT facilities appropriately and effectively

h. comply with the licensing and copyright conditions of software, equipment and electronic resources made available as part of the University IT facilities and services

i. prevent loss or theft of IT equipment containing University information, particularly personal data or information that is sensitive and confidential: encrypt devices storing University personal data , do not leave unattended in public, prevent casual access using PIN, password or device lock, protect the device when not in use

j. report security incidents, actual or suspected breaches of this policy, and loss, theft or compromise of IT equipment storing University Information via the CSD self-service portal: https://servicedesk.liverpool.ac.uk. Report personal data loss incidents 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 User IT accounts are informed by the start and end dates in the HR and Student Records systems. Access to IT accounts 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;
- return University purchased IT equipment (in reasonable working condition), information and resources to the University; and
- ensure any of their own data (that they wish to keep) 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 or University Policy and Regulations.

2.3.2 not create, 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 account password.

2.3.4 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 or the IT facilities of other organisations.

2.3.5 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 disrupt the work of other Users or the correct functioning of the University IT facilities.

2.3.6 not tamper with networking or other CSD centrally provided equipment, or continue to use systems, hardware or devices that CSD have requested cease or have disconnected.

2.3.7 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, offence, harassment, bullying, discrimination, victimisation, needless anxiety or persistent nuisance to others

f. corrupt, destroy or disrupt other users' data or deny and disrupt services to other users, for example: unnecessary or trivial messages, chain, junk mail or unsolicited bulk or marketing email (spam)

g. plagiarise or infringe the copyright, licence terms, trademark or proprietary rights of another person or organisation

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 UK Connection Policy (See Related Documentation section) such as use of IT facilities for non-University commercial purposes.

2.4 Exceptions

2.4.1 In the event of unexpected absence where information or correspondence isn't 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 CSD 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

appropriate risk management procedures including: health & safety duty of care, appropriate legal and 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 CSD self-service portal: https://servicedesk.liverpool.ac.uk.

3.0 Policy Compliance

3.1 Provision and Monitoring of IT Facilities

The Computing Services Department (CSD) is the System Owner for University centrally managed IT facilities on behalf of the University of Liverpool. This includes responsibility for ensuring measures are in place to achieve an appropriate balance of confidentiality, integrity, availability and resilience of information and IT facilities with the available resources.

CSD will communicate key system and service announcements to all Users.

CSD logs all use of University IT facilities using automated software and manual processes to carry out capacity planning, to check performance of a system, to investigate malicious activity against a system or machine. Logs are not actively monitored down to an individual level. Monitoring is only carried out to the extent permitted or as required by law, in accordance with 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 (system maintenance and administration)
- To investigate, detect or prevent the unauthorised use of the IT facilities
- To monitor whether use of the IT facilities is legitimate and in accordance with 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, an IT Activity Investigation Request Form must be completed. IT activity investigations should only be initiated where there is a specific and justified need in relation to an allegation of misuse or policy breach, an IT security incident or formal request from 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, policy of student conduct and discipline, academic or research misconduct policies)

- appropriately authorised by the Head of Department or other authorised role holder and the Director of the Computing Services Department
- managed in accordance with University disciplinary and / or misconduct policies and procedures, and be subject to clear scope, approval, documentation and evidence handling procedures in accordance with the CSD Cyber Security Incident Response Team (CSIRT) Terms of Reference to ensure the findings are admissible in a formal dispute or legal process (See Related Documentation section).

3.3 Breach of Policy

Misuse of IT and communications systems can damage the University and its reputation. Breach of this policy may be dealt with under the University's polices 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, CSD CSIRT will, on behalf of the University, exercise discretion to:

- Restrict or terminate a User's access to University IT facilities
- Take down content
- Disconnect systems or 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, in accordance with the staff disciplinary policy, policy of student conduct and discipline, academic misconduct or research misconduct policy.
- Refer information to the police, regulatory body or other law enforcement agency in connection with a criminal investigation.

4.0 Related Documentation

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

- JANET (UK) Connection, Security & Acceptable Use Policies
- Information Security
- CSIRT (Cyber Security Incident Response Team) Terms of Reference (in draft)
- Data Protection
- Social media compliance policy
- Staff related Policies including Staff Disciplinary
- Research related Policies including Research Misconduct
- Student related Policies including Student Conduct & Discipline and Academic Integrity

Guidance

- Operational Access Request, IT activity Investigation Request and Internet Exception forms are part of the Information Access Catalog located within the CSD self-service portal: https://servicedesk.liverpool.ac.uk >Requests> Information Access forms
- Computing Services Department webpages: https://www.liverpool.ac.uk/csd

5.0 Policy Document Control

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Information Security Officer (Christa Price)	Major revision of IT Regulations into IT Acceptable Use Policy (AUP). This AUP will be supported by the CSIRT Terms of Reference. 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 Formal Senior Leadership Team: 22/06/20 Council: 07/07/20
John Cartwright, Chris Woof, Steve Aldridge, Sue 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 the Computing Services Department. The Director of CSD has the authority to issue and communicate policy on IT facilities including information security priorities. The Director of Computing Services has delegated responsibility for the day to day implementation and communication of the policy to the Information Security Officer and will be supported by CSD teams.		
Policy Enquiries	Please direct any queries about this Policy to the CSD self-service portal: https://servicedesk.liverpool.ac.uk		
Policy Review			
Review due:	Annually by July 2021		
Document Location:	CSD webpages https://www.liverpool.ac.uk/csd/regulations/ University Policy Repository (under development)		
** The Owner & Author are responsible for publicising this policy document.**			