IT Acceptable Use Policy

2023-2024

Edge Hill University

Contents

Summary 3

Glossary of Terms 3

Purpose 3

1. Acceptable and unacceptable use 3

2. Access to Janet, the Internet, other networks and online services 5

3. Research 5

4. Personal Use 5

5. Email, messaging, social media and other online forums 6

6. Liability 7

7. Compliance and Illegal Material 7

8. User IDs and Passwords 7

9. Logging and Monitoring 8

10. Security, Privacy and Access 8

11. Staff Email Services, Retention and Recovery 9

12. Software Licensing, Copyright and Installations 10

14. Use of personal IT equipment and Eduroam wireless services 11

15. Removal of IT Equipment, Software or Information 12

16. Suspension of Access 12

Key to Relevant Documents 13

Endmatter 14

Summary
This Policy aims to provide clear information for our community on what constitutes acceptable and unacceptable use of the University IT infrastructure, networks, computing devices and online services. It provides examples to enable greater understanding of what and how users can safely access our online systems and help to ensure IT facilities and services remain secure, accessible and available for all.

Glossary of Terms

Multi Factor Authentication (MFA)
An IT security technology that requires two or more distinct mechanisms to validate a user's identity. MFA can prevent unauthorised access to IT applications and sensitive data, and helps defend against identity theft, cyberattacks and data breaches.

Purpose

The University IT infrastructure, systems and services aim to contribute to the high-quality learning, living and working environment, to facilitate academic, research and business functions of the University, and to serve the needs and interests of our students, staff and wider IT user community.

The purpose of this Policy is to state what constitutes acceptable use of the University IT infrastructure, computing devices and online services. It seeks to protect the University, its students and staff, partners and those using our IT facilities from inappropriate, non-compliant or illegal actions, and to provide guidance on the informal and formal means of dealing with unacceptable or inappropriate use, should it occur.

This Policy applies to all members of staff including associate and temporary staff, researchers, registered students, contractors, visitors to the University, and to those using and/or accessing any element of the University IT infrastructure, systems and services, from on or off campus. It is the responsibility of every user of any University IT resource(s) to read and adhere to this Policy.

1. Acceptable and unacceptable use

1.1 Use of the University IT infrastructure, systems and services for any activity which may reasonably be regarded as unlawful is not permitted.

1.2 Edge Hill University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". Staff, students and visitors using

University IT facilities must not create, download, store or transmit any unlawful material, or material that is indecent, offensive, defamatory, threatening discriminatory or extremist. The University reserves the right to monitor and/or block access to such material. If a member of the University community believes they may have encountered such material, they should report this immediately to the designated Safeguarding Officer.

1.3 University IT facilities or networks must not be used for any of the activities:

a. Creation, download, storage or transmission, or causing the transmission, of:

i. Offensive, obscene or indecent images or other material, or any data capable of being resolved into obscene or indecent images or material

ii. Material with the intent to cause annoyance, inconvenience or needless anxiety

iii. Material with the intent to defraud

iv. Defamatory material

v. Extremist material, or material with the potential to radicalise themselves or others

vi. Material such that this infringes the copyright of another person

vii. Unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe

b. Deliberate unauthorised access to information, systems, services or resources

c. Deliberate activities having, with reasonable likelihood, any of the following characteristics:

i. denial and/or disruption of services

ii. corruption or destruction of data

iii. violation of privacy

iv. use of prohibited hardware, software or services

v. the introduction of viruses, malware or other harmful software

vi. wasteful or other misuse of University IT infrastructure, network services and/or resources.

2. Access to Janet, the Internet, other networks and online services

2.1 Janet is a high-speed network for the UK research and education community. Operated by Jisc, the Janet network provides essential ISP services to most UK universities. The Janet Network Connection Policy and the Janet Acceptable Use Policy define the acceptable use and legal requirements, and failure to comply with these can result in services being withdrawn from the University. https://community.jisc.ac.uk/library/janet-services-documentation/janet-policies-and-legal-requirements

2.3 Where the University network, or the Janet network, is used to access another network or online service, any abuse of that network or service will be regarded as unacceptable use under this Policy.

2.3 Any deliberate activity that is likely to damage the reputation of the University and/or members of the University community, is unacceptable, will be investigated as and may result in disciplinary action.

3. Research

3.1 It is recognised that, during their work or research, registered users of the University may have a requirement to view, download, create or transmit material that would normally be defined as unacceptable use. In the case of properly authorised, supervised and lawful research purposes, individuals may apply for access using the University's Application to access Sensitive Content Form and obtain the authorising signature of the relevant PVC Dean / Director, prior to submission to the Research Office for consideration by the Ethics Committee. The Ethics Committee may authorise the necessary access, for a limited period, if deemed appropriate. Individuals must understand that an Application to access Sensitive Content does not sanction the committal of acts that are illegal.

4. Personal Use

4.1 Reasonable personal use of University IT facilities, infrastructure and services is a permitted privilege, not a right, on the understanding that personal use:

a. is lawful and complies with the University's rules, regulations, policies and procedures, this Policy, the University Information Security Policy and the JANET Acceptable Use Policy

b. is not detrimental to the main purpose for which the facilities are provided

c. does not interfere with the performance of an individual's duties

d. does not take priority over an individual's work or learning responsibilities

e. is not of a commercial or profit-making nature, or for any other form of personal financial gain

f. is not of a nature that competes with the University in business

g. is not connected with any use or application that conflicts with an individual's obligations, contractual or otherwise, to the University

h. does not incur unwarranted expense on the University

i. does not in any way have a negative impact on the University.

4.2 For the purposes of monitoring (see Section 10), all University email is deemed to be business related communications, unless specifically identified as 'Personal' in the title / subject line.

5. Email, messaging, social media and other online forums

5.1 Email, messages, posts and images, including those on social media and other online forums, may be read by others and content could find their way into the public domain. Inaccurate or improper statements, posts and/or inappropriate images, may be disclosed, are admissible in legal proceedings, and may give rise to personal or corporate liability. The following activities are not permitted:

a. Posting of extremist, obscene or offensive comments, or otherwise objectionable material (including libellous, unlawful, defamatory, racist, sexist, homophobic, harassing, harmful, abusive, threatening, or visual sexual references);

b. Posting of material that may violate, plagiarise, or infringe on the rights of third parties including copyright, trademark, trade secret, privacy, personal, publicity, or proprietary rights;

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

6. Liability

6.1 When using University IT facilities and / or services each user agrees that the University shall have no liability for the loss or corruption of any user file or files, information or data; and/or the loss or damage to any user owned equipment, devices, systems or other assets resulting from the individual's use of the University IT infrastructure and services. The University shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of these services, or with any delayed access to, or inability to use these services.

7. Compliance and Illegal Material

7.1 Under UK law the University has a legal responsibility for the content and nature of all materials stored on, accessed and/or transmitted via the University IT infrastructure, and has therefore adopted standard procedures in place to log and verify reports of potentially illegal material. The University will not endorse the committal of acts that are illegal, and where illegal material is suspected as having been viewed, downloaded, created, stored or transmitted, the information will be immediately forwarded to the law enforcement agencies for investigation.

8. User IDs and Passwords

8.1 Registered users must not disclose their passwords and must take all reasonable precautions to ensure that their password remains confidential. The use of another individual's User ID and password is not permitted under any circumstances. Any individual who discloses their password to another will be held responsible for any improper actions committed under that User ID and, in circumstances where further breaches of the AUP occur, accountability may fall equally on the holder of the account, as on the individual using the account at the time. Where a temporary password is issued, it must be changed immediately to a secure password known only to the individual; failure to do so will create a security risk.

8.2 A secure password or passphrase should be a minimum of eight characters in length and use a combination of alphabetic (upper and lower case), numeric and special characters.

8.3 Where available, multi-factor authentication must be used on all University and third-party services.

9. Logging and Monitoring

9.1 As defined under The Regulation of Investigatory Powers Act 2000, the University can monitor electronic communications, telecommunications systems and activity across the IT infrastructure and network services to capture evidence of transactions, ensuring regulatory compliance, detection of crime or unauthorised use, and for system monitoring to ensure the operational effectiveness of IT services. University systems automatically record all registered user account logins, system accesses, email and internet activity on and across the University IT infrastructure. These records may also be used to aid investigation of alleged disciplinary or criminal misconduct, and the University will comply with lawful requests for information from government and law enforcement agencies.

10. Security, Privacy and Access

10.1 Individuals should be aware that electronic communications and transactions are vulnerable to potentially malicious activity and security breaches during transmission and can be intercepted, read, lost, redirected or amended. It is the responsibility of the individual to appropriately check communications and transactions, files and data, to ensure it is from an identifiable and reliable source. Whilst the University shall take reasonable measures to reduce the risk of malicious activity and/or vulnerability to security breaches, the University shall not be held responsible for any loss or damage resulting from an individual's use of, and/or access to, University IT infrastructure and services.

10.2 All registered users need to be aware that the automated monitoring of their usage may reveal sensitive personal data about the individual. By using and/or accessing the University IT infrastructure and services, registered users consent to the University processing any sensitive personal data (in line with the principles of the Data Protection Act and GDPR) which may reveal unacceptable or illegal activity.

10.3 Network account access privileges of staff will normally start on their first day of employment with the University and be terminated on their last day of employment - as defined by the employment dates recorded on the central HR system. The staff network account and all account content will typically be marked for permanent deletion 120 days after the last day of employment.

10.4 Network account access privileges of students will normally start from when their Student Record is created (i.e. prior to, and to facilitate, Online Enrolment). Student accounts will typically be terminated within 120 days of their course instance end date – and/or as defined by the student 'status' and dates held on the central Student Records System. *S*tudent network accounts and all account content will be marked for permanent deletion 12 months after the course instance end date.

10.5 Access to another user's email account or home directory files is not permitted without the individual's explicit prior consent, or where the individual self-enables 'proxy' access to other named user(s). If this is unavailable, and only in exceptional circumstances, a PVC / Dean / Director should submit a documented case with defined timescales for consideration by the DVC, to be approved (or otherwise) by the VC. Should access be granted, the individual must be informed that access has been granted during their absence by the relevant PVC / Dean / Director. In addition, access will be time limited to a maximum of four weeks, or shorter period as appropriate to the specific documented circumstances. Access to email and/or home directories may be granted as part of a disciplinary or criminal investigation, where similar approvals have been confirmed.

11. Staff Email Services, Retention and Recovery

11.1 All University staff are provided with access to an individual MS Office 365 Outlook Email and Calendaring account via an externally hosted service delivered to the University under license directly by Microsoft. Within this MS O365 Cloud-based environment, all data is securely stored offsite within Microsoft's Data Centres - as per the Terms and Conditions of the License Agreement.

11.2 The University operates a two-year Retention Policy on all items within individual (active) staff O365 accounts - this includes, but is not limited to, Email items, Calendar entries, Groups and Tasks. The Retention Policy applies to all folders and all subfolders within an individual O365 account - including Inbox, Sent Items, and any custom folders created by the staff member. Any items over two years old will be automatically moved by the system to the 'Deleted Items' folder.

All items located in 'Deleted Items', be they user-initiated and/or automatically by the system (as described above), will be retained for a maximum of 30 days, after which they will remain 'user recoverable' for a further 30 days. After this 'user recoverable' period, all items will be automatically purged and permanently deleted from the system and will not be recoverable. By default, shared University mailboxes will have a 30 day retention period.

11.3 Any important O365 business correspondence and/or documents required beyond the automated retention period, including email and email attachments, should be exported and stored outside of the O365 environment in an appropriate University-managed repository (be it electronic and/or hardcopy). The University does not permit the auto-forwarding to, or permanent storage of, any University business correspondence, email or attachment to non- University managed email systems or services (including but not limited to personal email accounts, online file stores, etc.).

12. Software Licensing, Copyright and Installations

12.1 The use of software products is limited to the purposes defined in the software license agreement - typically for teaching, research, personal educational development, administration and management of University business. All registered users are responsible for abiding by the relevant terms and conditions and, in some cases, software licenses may only be used on University IT equipment covered by that specific license agreement. Under no circumstances should University users copy or distribute copies of any University licensed software. The use of unlicensed software is illegal and, unless formally advised to the contrary, it is to be assumed that all software products are subject to Copyright Law.

12.2 The downloading, storing or transmitting of copyrighted material, including electronic texts, music and video files, is not permitted. It is also illegal under the 'Copyright, Designs and Patents Act (1988)' to reuse or distribute copyrighted content without the documented permission of the copyright holder, including all Edge Hill University lecture capture recordings and content. The University will perform checks across all IT systems and services for peer-to-peer file-sharing software and files suspected to contain copyrighted material. Where copyrighted material is suspected, the user's account will be disabled, and the files removed pending further investigation.

12.3 Registered users are not permitted to install any software or executable files on the University IT infrastructure without the prior formal consent of a HoD and IT Services representative. IT Services perform regular checks and where files or software of this type are found, the user's account will be disabled, and the files removed pending further investigation.

14. Use of personal IT equipment and Eduroam wireless services

14.1 The IT infrastructure supports a range of network services to underpin the academic and business requirements of the University, and to deliver a portfolio of online services for registered users. For the purposes of this Policy, these network services shall be categorised as either 'wired' (i.e. a physical connection between networked device via a cable) or 'wireless'. Only authorised IT Services staff are permitted to connect and disconnect University provided IT devices and telephony equipment to the wired network, and under no circumstances should personal / user owned IT devices be connected to the University wired network infrastructure without prior approval. Any individual found to have connected a device to, or disconnected from, the wired network infrastructure will be held responsible for any loss or damage to University IT infrastructure and services, and therefore may be pursued for financial liability.

14.2 Registered users are permitted to use personal / user owned IT devices on University premises, and to connect these to the 'eduroam' wireless network. The eduroam service provides connectivity on all Edge Hill University campus sites, and also offers wireless connectivity at many other participating institutions https://www.ja.net/products-services/janet-connect/eduroam

14.3 Before any personal electrical device is connected into the campus electrical distribution system, individuals should ensure they are able to demonstrate that their equipment has been the subject of an appropriate visual inspection as defined by the Electricity at Work Regulations Approved Code of Practice. Individuals using personal / user owned IT devices to access or connect to any element of the University IT infrastructure and services do so on the understanding that this is done at the individual's own risk.

14.4 Staff wishing to access University O365 email services and/or other University systems from a personal / user owned device (including smartphones and tablets) must use University approved clients (or apps) and must adhere to the University Multi Factor Authentication requirements, may be required to pre-

register their device(s), and should accept the right of the University to selectively remove / remotely wipe any University data from the device where this is deemed appropriate (ego loss / theft of device, staff leavers, etc). The University O365 email services will not support legacy Outlook clients or older smartphone 'email apps' (such as those using IMAP and/or POP), and instead staff should ensure their devices are regularly updated to use the latest MS Outlook App available from the online Store(s).

14.5 The University accepts no responsibility for any loss or damage to user owned IT devices or data.

15. Removal of IT Equipment, Software or Information

15.1 The removal of University IT equipment, telecommunications devices, software or information is not permitted without prior formal authorisation from the appropriate University authority – typically PVC-Dean, Director and/or HoD. All University IT-related 'assets' authorised for removal from campus should be formally recorded by the department / faculty and reviewed annually. IT equipment removed without authorisation may be viewed as theft and will be investigated.

16. Suspension of Access

16.1 All users have a responsibility to adhere to this Policy and the associated policies referenced therein. Where a breach has been identified, or infringement suspected, suspension of access to IT facilities will be immediately implemented to enable the incident to be investigated. Where it has been proven that a breach has occurred, formal disciplinary proceedings may be implemented.

Key to Relevant Documents

Relevant University documents and UK legislation which relate to and/or govern the provision and use of IT facilities include:

Edge Hill University

- Information Strategy
- Information Security Policy
- Privacy Policy
- Records Management Policy
- Data Security Breach Policy
- Data Protection Policy

UK Regulations and Acts of Parliament

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Copyright, Designs & Patents Act 1988
- Copyright and Trade Marks (Offences and Enforcement) Act 2002
- The Telecommunications Act (1984)
- The Electronic Communications Act (2000)
- Obscene Publication Act 1959 & 1964
- Protection of Children Act 1978
- The Defamation Act (1996 and 2013)
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter Terrorism and Security Act 2015
- Human Rights Act 1998
- Equality Act 2010
- Privacy and Electronic Communications Regulations 2003

Endmatter

Title	IT Acceptable Use Policy
Policy Owner	Director of IT Services
Approved by	Information Strategy Group
Date of Approval	7th June 2023
Date for Review	June 2024