Edge Hill
University

IT Acceptable Use Policy

1. Scope and Purpose

This IT Acceptable Use Policy (AUP) applies to all University students and staff including temporary and associate staff, researchers, contractors, and 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.

The purpose of this policy is to protect the University, its students and staff, partners and those using our IT facilities from illegal, inappropriate or damaging actions. The University IT infrastructure, systems and services are to be used for academic and business purposes in serving the interests of the University, and of our clients and customers in the course of normal operations. It is the responsibility of every University IT user to read and adhere to this AUP, the University Information Security Policy , the JANET AUP and applicable UK laws (a non-exhaustive list of which is provided in Section 16 of this Policy). Infringements and breaches of these regulations may result in disciplinary or legal action.

2. Unacceptable Use

In accordance with UK law, the use of the University IT infrastructure, systems and services for any activity which may reasonably be regarded as unlawful is not permitted.

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

In addition, the University IT and network infrastructure must not be used for any of the activities described below (this list of unacceptable activities is not necessarily exhaustive):

a. Creation, download, storage or transmission, or causing the transmission, of:
   i. Offensive, obscene or indecent images, data 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 networked facilities or services.

c. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
   i. wasting staff effort or networked resources;
   ii. corrupting or destroying other users' data;
   iii. violating the privacy of other users;
   iv. disrupting the work of other users;
   v. denying service to other users;
   vi. continuing to use an item of software or hardware after IT Services has requested that use cease;
   vii. other misuse of University IT infrastructure, services and resources, such as the introduction of "viruses" or other harmful software.

3. Access to JANET, Other Networks and Services

"JANET" is the name given both to an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK higher and further education and research community, and is maintained primarily to support education and research within the UK public sector. The JANET Acceptable Use Policy defines acceptable and unacceptable use, and failure to comply with may result in services being withdrawn from the University. It is the responsibility of every University IT user to read and adhere to the JANET AUP. Registered users must not 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. Where the University network is being used to access another network or service, any abuse of the acceptable use policy of that network will be regarded as unacceptable use. Any deliberate activity as described in Section 2 of this AUP, where applied to a user of that network, will also be regarded as unacceptable. Any activity that is likely to damage the reputation of the University, and/or of the University IT infrastructure and services, will also be regarded as unacceptable may result in disciplinary or legal action.

4. Research

It is recognised that, in the course of 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 IT Acceptable Use Policy Waiver 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 IT AUP Waiver does not sanction the committal of acts that are illegal.

5. Personal Use

The University permits the reasonable personal use of its IT facilities, infrastructure and services as a privilege, not a right, on the understanding that personal use:

a. is lawful and complies with the University's rules, regulations, policies and procedures and, in particular, this AUP, the University Information Security Policy and the JANET AUP;
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.

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

6. Social Networking Sites, Email, Blogs and Online Forums

Users should be mindful of the content of electronic messages or posts, including those on social networking sites, forums and virtual learning environments, as incorrect or improper statements can give rise to personal or corporate liability. Electronic messages and posts may be read by others, content could it find its way into the public domain, and may be disclosed (and is admissible) in legal proceedings. Deletion of posted content does not necessarily mean that an electronic message or post is irretrievable.

The following activities are not permitted:

a. Posting of extremist, obscene or offensive comments, or otherwise objectionable material (including but not limited to 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.

7. Liability

In using the 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.

8. Compliance and Illegal Material

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.

9. User IDs and Passwords

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. Registered users should select a secure password by using a combination of alphabetic and non-alphabetic characters; avoiding the use of real names or words, or the use of sequences of numbers or letters.

10. Logging and Monitoring

As defined under The Regulation of Investigatory Powers Act 2000, the University monitors electronic communications, telecommunications systems and activity across the IT infrastructure and network services for the purpose of recording 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.

11. Security, Privacy and Access

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 vulnerable 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.

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) which may reveal unacceptable or illegal activity.

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 per the dates held on the central HR System. The staff network account and all account content will be permanently deleted 120 days after the last day of employment.

Network account access privileges of students will normally start from when their Student Record is created (prior to, and to facilitate, Online Enrolment). Student accounts will typically be terminated within 30 days of withdrawal and/or their course instance end date - as per the student 'status' and dates held on the central Student Records System. *S*tudent network accounts and all account content will be permanently deleted 12 months after the course instance end date.

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 4 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.

12. University Staff Email Services, Retention and Recovery Policy

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

The University now maintains a two-year Retention Policy on all items within individual staff Outlook accounts - this includes, but is not limited to, Email Items, Calendar Entries, and Tasks. The Retention Policy applies to all folders and all subfolders within an individual mailbox, 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.

Any important Outlook business correspondence and/or documents required beyond the automated two year retention period, including email and email attachments, should be exported and stored outside of the Outlook 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 filestores, etc.).

13. Software Licensing and Copyright

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.

The downloading, storing or transmitting of copyrighted material, including electronic texts, music and video files, is not permitted (see Section 2.5). 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. Disciplinary and/or legal action may follow.

14. Software Installations and Executable Files

Registered users are not permitted to install any software or executable files on the University IT infrastructure without the prior formal consent of a senior 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, and disciplinary action may follow.

15. Bring Your Own Device, use of personal IT equipment & Eduroam

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' (ie 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.

Registered users are permitted to use personal / user owned IT devices on University premises, and to connect these to the 'eduroam' wireless network. Eduroam (https://www.ja.net/products-services/janet-connect/eduroam) will not only provide connectivity on Edge Hill University campus sites, but also offers wireless connectivity at many other participating educational institutions.

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.

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

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 and/or apps, 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 (eg loss / theft of device, staff leavers, etc). The University O365 email services will not support legacy Outlook clients or 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).

16. Removal of IT Equipment, Software or Information

The removal of University IT equipment, telecommunications devices, software or information is not permitted without prior formal authorisation from the appropriate University authority. University IT-related 'assets' removed without authorisation may be viewed as being stolen, and may result in disciplinary proceedings.

17. Legislation (and associated polices)

Applicable laws, primary Acts of Parliament and policies which relate to and/or govern the provision and use of IT facilities include:

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
** This list is not exhaustive and will be subject to change **

18. Suspension of Access

All users have the responsibility to adhere to this AUP 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.