Keele UNIVERSITY

IT Acceptable Use Policy

Table of Contents

1. INTRODUCTION

1.1 The aim of this Policy is to help ensure that the University's IT facilities can be used safely, lawfully and fairly.

1.2 The IT Acceptable Use Policy (AUP) aims to:

- Ensure users have proper awareness and concern for the security of IT resources and adequate appreciation of their responsibilities when those resources are used;
- Set out the acceptable use of University IT resources;
- Ensure that users are aware of their obligations when using IT resources;
- Ensure users are aware of their accountability and that failure to abide by this policy may be a disciplinary matter as part of the student regulations or the employee contract terms;
- Ultimately, failure to comply with the policy could result in dismissal, cancellation of contract, agreements or legal action.

1.3 By accessing or using the IT facilities or acknowledging that you have read and understood the Policy when prompted, you agree to be bound by this policy, including all documents referred to within it. All staff and students will be required, as part of the user set up and authentication processes, to acknowledge that they have read and understood the policy.

2. PURPOSE

2.1 The University IT resources provided for academic purposes and University corporate business are extremely valuable assets which are relied upon for the delivery of University services.

2.2 This policy is designed to support all areas of the University when using IT resources, whether on or off campus. The intention is that this policy will enable the University to carry out its activities, by protecting and preserving University resources at the appropriate level.

2.3 The acceptable use of specific IT resources will be detailed within the main body of the policy to set out what your responsibilities and behaviours must be.

3. SCOPE

3.1 Who is covered by this policy?

3.1.1 This policy applies to people, denoted as 'users', using Keele University's IT resources as detailed in section 3.1.2, 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, on behalf of, or in partnership with the University;
- Members of Council and associated committees, 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; recruitment agents;
- Students and staff from other institutions logging on using Eduroam;
- University tenants using University IT Facilities;

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

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

3.2 What IT resources are covered by this policy?

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

- Traditional desktop computers e.g. desktop PCs, Apple Macs or other Apple computers and laptops;
- Peripherals e.g. printers, copiers, scanners and multi-function devices;
- Meeting room technology e.g. touch/smart screens, multi-function displays, wireless projectors and associated software;
- Mobile devices, e.g. smartphones (IOS and Android and other mobile operating systems), tablets, iPads, MacBooks and other 'smart' devices;
- Other networked devices such as games consoles and IoT devices;
- Networks with wired, wireless, VPN with or without internet connections;
- Email and instant messaging, social networking or collaboration services e.g. blogs, vlogs, chat, forums, Facebook, Twitter, YouTube, Instagram, etc. This includes the use of personal email and social media accounts using University IT resources.
- Application software, services and data including databases;
- Removable and optical media, such as CDs, DVDs, Blu-Rays and flash memory e.g., USB memory sticks;
- Access to resources using personal devices, e.g., devices not provided by the University.
- Any piece of infrastructure or medium, internal and external in the cloud or on premise used in the transmission and processing of data for university business.
- Resources accessed via personal devices as defined in the Bring Your Own Device (BYOD) Guidance.

3.3 Agile working

3.3.1 The principles and requirements outlined in this policy must be applied when working in an agile manner either on or off campus.

3.3.2 When working off campus you should maintain the security of the university's information assets (the data and information you use for university activities such as teaching and learning, professional services, or research for example) by using IDS-provided Cloud services such as Microsoft365 (e.g., Teams and OneDrive), AWS services, and other approved applications, systems, and services.

4. POLICY

4.1 This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by Jisc[1], the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement.

4.2 Background and Definitions

- "University" refers to the University of Keele
- "University Network" refers to active computer systems, services and facilities provided within the "keele.ac.uk" domain.
- "University User Community" includes anyone who is authorised to use the University Network.
- "Users" includes members of the University User Community and users of any other network.
- "JANET" is the name given to the collection of networking services and facilities which currently support the communication requirements of the UK education and research community.
- "User Organisation" is any organisation authorised to use Janet. JANET is maintained to support teaching, learning and research. Only organizations whose predominant use of JANET falls into these categories, or whose use is approved by the JISC, will be permitted to make a connection to JANET, whether directly or via another organization itself connected to JANET.
- The University is an authorised JANET User Organisation. As such it has the responsibility to ensure that members of its own user community use JANET services in an acceptable manner and in accordance with current legislation.
- As a consequence of being an authorised JANET User Organisation all members of the University user community are subject to the JANET Acceptable Use Policy.
- In addition, all members of the University User Community are subject to the Keele IT Acceptable Use Policy which is an adjunct to the Janet Acceptable Use Policy and which is specified in this document.
- Breaches of either the Janet Acceptable Use Policy or the Keele IT Acceptable Use Policy will be regarded as disciplinary offences and dealt with under the University disciplinary procedures.

4.3 The University has an obligation to comply with the following legislation:

- Data Protection Legislation (DPA2018, UK GDPR, Privacy and Electronic Communications Regulations 2003 including Data Subject Access Requests)
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988
- The Copyright and Rights in Performances (Quotation and Parody) Regulations 2014
- Computer Misuse Act 1990
- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance: for Higher Education Institutions in England and Wales
- Public Interest Disclosure Act 1998
- Defamation Act 1996
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- Equality Act 2010 – including ensuring adherence with web accessibility guidelines as defined by the Web Content Accessibility Guidelines (WCAG) 2.2 (https://www.w3.org/TR/WCAG22/)
- Other related legislation that may influence this policy

[1] Jisc are the UK higher, further education and skills sectors' not-for-profit organisation for digital services and solutions. They champion the importance and potential of digital technologies for UK education and research

4.4 Acceptable Use

4.4.1 Subject to the following paragraphs, the University's IT resources may be used for any legal activity that is in furtherance of the purpose, aims and policies of the University, and that is used subject to the associated policies and Codes of Practice as listed in this document.

4.5 Unacceptable Use

4.5.1 The University's IT resources **may not** be used for any of the following:

- the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- the creation or transmission of defamatory material;
- the transmission of material such that this infringes the copyright and intellectual property rights of another person;
- the unauthorised transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
- deliberate unauthorised access to user accounts, facilities or services accessible via the University network;
- deliberate activities with any of the following characteristics:
  - corrupting or destroying other users' data;
  - disrupting the work of other users;
  - using the University network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
  - continuing to use an item of networking software or hardware after the University has requested that use cease because it is causing disruption to the correct functioning of the University network
  - other misuse of the University network or its networked resources, such as the introduction of "viruses".
- the creation or transmission of any material which could bring the University into disrepute;

4.5.2 Where the University network is being used to access any other network including JANET, the acceptable use policy of that network must be upheld.

4.5.3 Specifically, users are prohibited from:

- Uninstalling and/or reconfiguring antivirus, anti-malware, updates, any management or inventory tool deemed mandatory by IDS on University owned or managed devices;
- Attempting to disrupt or circumvent IT security measures by wilfully, and without prior written consent from IDS, installing software or hardware to counteract these measures;
- Storing Keele data and information; electronic files, extracts, research data for example, on any Cloud based service or personal device (must be stored on Keele owned Cloud services such as Teams, OneDrive, AWS or Azure Cloud) unless with specific and directed approval from the DPO or IDS;
- Implementing devices, software or services designed to anonymise or disguise the identity of the device or user account;
- Using their University account after the period of employment or service;
- Intentionally or recklessly introducing any form of malware, spyware, computer virus or other potentially malicious software e.g. by illegally downloading games;

- Using any form of peer to peer or file sharing service with the intention of illegally obtaining copyright material using any University equipment or personal equipment connected to University infrastructure;
- Using any form of software or hardware or service for personal monetary gain at the expense of the University, this includes crypto-mining;
- Sharing personal account credentials with another user;
- Leaving devices unattended and logged in without locking the screen e.g. when locating a book in the Library;
- Using personal email accounts instead of a University Staff email account to conduct University business, or automatically forwarding emails from a staff email account to a personal account (except where permission has been sought to use alternative email addresses in the case of a major cyber incident);
- Using Keele IT credentials (user ID and password) in conjunction with personal use e.g., setting up bank accounts or shopping accounts unless specifically authorised to do so by **Procurement;**
- Wilfully introducing malicious software to the University infrastructure or devices whether they be University owned or personal to promote any data-interception, password-detecting or illegal activity broadly defined under the term 'hacking';
- Setting up servers or services and / or using any aspect of Keele IT infrastructure for services that are not of a Keele business or academic nature or present a Cybersecurity risk Seeking to gain unauthorised electronic access to restricted areas of the University's network or infrastructure;
- Seeking to gain unauthorised physical access to sensitive areas of University infrastructure or network with malicious intent;
- Access or attempted access to data when the user knows or ought to know that they do not have access;
- Connecting network equipment including but not limited to; network switches, routers, wireless access points, network monitoring tools or impersonating network services provided by Keele University;
- Installing devices with specific hacking or monitoring tools with the intent of performing testing or monitoring of network traffic, even for the purpose of teaching without prior written permission from IDS;
- Installing and operating any service or device using the University network, infrastructure, desktop or mobile equipment or other peripheral resources for monetary gain;
- Transfer any University data without appropriate permission.

4.6 Usage Exceptions

4.6.1 There are several exceptional activities, usually in relation to academic freedoms, that may be carried out using University IT resources that could ordinarily be considered as unacceptable use and therefore would be in breach of this policy.

4.6.2 Approval of these exemptions will be undertaken by the CIO or their designated, authorised nominee(s) in consultation with other senior staff within the University as required.

Examples may be:

- Research involving defamatory, discriminatory or threatening material
- The accessing or use of images which may depict violence or may otherwise be restricted
- The study of hate crime
- Terrorism related material

- Research into computer intrusion techniques
- Access by Faculties for research, learning or understanding purposes

5. MONITORING AND AUTHORISED ACCESS

5.1 IT Network use and communications may be monitored for the business purposes of the University as permitted by UK legislation, as set out at 2.1 above. The legislation allows the interception of network traffic without consent for purposes such as:

- recording evidence of transactions
- ensuring regulatory compliance
- detecting crime or unauthorised use

5.2 Documents and or communications could potentially be released to requestors if considered in the public interest under the Freedom of Information Act (2000).

5.3 In line with its obligations under the Data Protection Act 2018 and UK GDPR, all data held by the University within its IT systems is subject to search and retrieval in the processing of an Individual Rights Request, such as a Subject Access Request.

5.4 Access to a user's email, files or documents related to the University's activities may also be granted to a line manager or authorised alternate if the user is unavailable for their normal duties for a period and the materials are necessary for the efficient operation of the University and / or disciplinary matters.

5.5 The University undertakes routine monitoring of activity of the network, attached devices (wired or wireless), infrastructure and software services both on premise and in the Cloud to ensure that it is operating correctly and to protect against the risk of harm from viruses, malicious attack and other known threats.

5.6 University and device ID's may be monitored to track location whilst on campus for the purposes of managing building occupancy and other University business requirements.

5.7 Keele maintains a Monitoring and Interception Policy which is available on Policy Zone.

6. CONSEQUENCES OF BREACH OF THE AUP

6.1 Minor breaches of this policy will be dealt with by IDS and a Staff user's line manager may be informed of the fact that a breach of policy has taken place.

6.2 More serious breaches of policy, or repeated minor breaches, will be dealt with under the University's disciplinary procedures. Disciplinary action may take the form of, but is not limited to:

- Withdrawal of computing facilities;
- Formal disciplinary sanctions including warnings, suspension or dismissal / expulsion;
- The imposition of a fine for students only.

6.3 More information can be found on the Staff HR and Student Regulation webpages.

6.4 Where appropriate, in consultation with the Secretary to Council and Chief Operating Officer, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

7. LIABILITY

7.1 The University has no obligation to retain a user's IT resources after their authorisation has ended beyond the retention periods set by the University.

7.2 Whilst every effort is made to prevent disruption to internet services, the University does not guarantee that an internet connection will be always available and cannot be held liable for any loss or damage (including consequential loss) caused by disruption to JANET, the University network and servers, or abuses by another user.

7.3 In using the IT resources each user agrees that the University shall have no liability for the correctness of results produced by such resources, the failure of the resources to produce results, loss or corruption of any use of file or files, information or data held and/or loss or damage to any user owned equipment, devices, systems or other assets resulting from the individual's use of the University's IT resources. As far as is permitted by law, the University shall not 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 resources. .

8. ROLES AND RESPONSIBILITIES

8.1 All users, as defined in paragraph 2.2.1, are required to abide by this policy and all associated guidance, processes and procedures aligned to this policy.

8.2 The CIO is responsible for reviewing and publishing this Policy and for providing policies, procedures, guidance, advice and training in support of it, and taking action pursuant to this Policy.

8.3 Directors or equivalent and Heads of School are responsible for ensuring that all staff and students within their area act in accordance with this Policy and established procedures.

9. RELATED POLICIES AND PROCEDURES

9.1 The issues covered by these regulations are complex and you are strongly urged to read all associated policies and guidance.

9.2 The following Policies and Codes of Practice must be read in conjunction with this Policy:

- Email Code of Practice
- IT Interception and Monitoring Policy

9.3 The following Policies, Guidance and Procedures should be read in support of this Policy. All documents are available in the Policy Zone :

- Data Classification and Handling Policy
- Data Protection Policy
- Information Governance Framework
- Information Security Policy
- Records Management Policy
- Records Retention Schedule
- Freedom of Information Act (FOI) Policy
- Vulnerability Disclosure Code of Practice

9.4 Details of IT related guidance can be found on the Information & Digital Services staff intranet pages (https://keeleacuk.sharepoint.com/sites/IDS)

10. REVIEW, APPROVAL & PUBLICATION

10.1 This policy is owned by the Information and Digital Services Directorate. As this policy governs the overall use of the IT infrastructure and details what behaviour is acceptable and what is not, the document will be reviewed annually by the Associate Director Projects and Service Assurance or the authorised nominee.

10.2 Approval

10.2.1 Approval will be secured from UEC, and Council.

11. PUBLICATION

11.1 Once fully approved, this policy will only reside in the Policy Zone . However, it is expected that links to the policy will be included in:

- The IDS SharePoint pages
- The Information Governance pages on the staff intranet

12. DOCUMENT CONTROL INFORMATION

Document Name	IT Acceptable Use Policy
Owner	Simon Clements – Head of Projects and Service Assurance
Version Number	v1.1
Equality Analysis Form Submission Date	NA
Approval Date	27/February/2023
Approved By	University Executive Committee
Date of Commencement	27/February/2023
Date of Last Review	27/February/2023
Date for Next Review	27/February/2026
Related University Policy Documents	Data Classification and Handling Policy, Data Protection Policy, Information Governance Framework, Information Security Policy, Records Management Policy, Records Retention Schedule, Freedom of Information Act (FOI) Policy, Vulnerability Disclosure Code of Practice
For Office Use – Keywords for search function	