Regulations for the use of IT Services and Resources

Reference code	IT Regs v2.8
Author/originator	Pro Vice Chancellor Digital Transformation
Approving Body	University Executive Board (UEB)
Last review date	30 – 04 - 2025
Next Review Date	28 – 07 - 2028
Ratified/authorised by	Pro Vice Chancellor Digital Transformation
Postholder/s responsible for review	Deputy Chief Information officer

Index

1. SCOPE

1.1 The regulations detailed in this document apply to anyone using IT Resources for any purpose at the University and its subsidiaries, including staff (temporary and permanent), affiliates, students, and visitors. This policy also covers personally owned equipment connected to the University's network or any of its services on University premises or an external location.

1.2 These Regulations should be read in conjunction with the following policies:

Document Name	Revision	Owner
Information Security Policy	1.1	Cyber Security - Service Manager
University Data Protection Policy	1.0	Head of Governance & Regulatory Affairs
User Access Control and Password Policy	1.1	Cyber Security - Service Manager
IT Hardware Policy	1.2	Deputy CIO
IT Software Policy	1.1	Deputy CIO
IT Email Policy	1.0	Deputy CIO
Personally Owned Device Policy	1.1	Cyber Security - Service Manager
Information Classification and Handling Policy	002	Information Governance Officer
Social Media Policy: Staff	N/A	Human Resources

1.3 The University provides access to services through the Internet via the Joint Academic Network (JANET). The University may only take advantage of the benefits of this access through clear adherence to the Acceptable Use Policy specified for all JANET users. All users should comply with these guidelines and not act in a way that puts the University out of compliance with the JANET Acceptable Use Policy.

1.4 Access to the University's resources is via authorisation. An authorised user is someone who has been granted legitimate access to the University's services through a valid University account. This account is provisioned on approval through the HR system or through enrolment as a student through the Student Records system.

1.5 It is the responsibility of all authorised users of University IT resources to ensure that IT is used for appropriate University purposes and in a manner that does not compromise the University, its employees, students or associated staff in any way. Any person using IT Resources must abide by these IT regulations.

1.6 To ensure that IT Resources are not abused the University retains the right to selectively monitor network traffic and to take any appropriate action if improper use is identified.

1.7 The University takes a strict approach to breaches of these regulations, which will be dealt with in accordance with the University's Disciplinary Procedures.

2. DISCLAIMER

2.1 The University undertakes to provide and operate its IT Resources with reasonable care and skill. However, the University accepts no liability for any loss or damage a user (authorised or otherwise) may suffer from any failure or malfunction of the University IT Resources or any parts thereof.

3. ADMINISTRATION OF THE POLICY & IT RESPONSIBILITIES

3.1 The administration of this policy comprising: monitoring, enforcing and taking preventative action is the responsibility of IT Services.

3.2 Members of IT Services will have delegated authority from the University Executive Board to take steps to protect the University.

3.3 IT Services will implement technical controls and procedures to enforce this Policy. It is the IT Services' responsibility to ensure that the technology estate (user devices, infrastructure, networks, applications & systems) remain secure and compliant with all relevant acts and laws.

4. AUTHORISED USER RESPONSIBILITIES

4.1 Members of the University and its subsidiaries will be authorised to use IT through appointment into a role or through enrolment on a course.

4.2 Authorised users may use IT Resources for the purpose of teaching, research, education and associated support.

4.3 Authorised use will also be provided to anyone working with or at the University, subject to the discretion of the University Executive Board or designated member thereof. This may include, for instance, staff from other HE organisations or from professional bodies.

4.4 Possession of an account is a privilege which may be revoked at any time at the discretion of the University Executive Board or designated member thereof.

5. LINE MANAGER RESPONSIBILITIES

5.1 Line Managers are responsible for ensuring that their teams—including contractors, temporary staff, and any third parties—are aware of and understand:

- This Policy and all supporting policies and procedures applicable to their work.
- Staff responsibilities for information security.
- How to access advice on information security matters.

5.2 Line Managers are also responsible for:

- Ensuring their teams complete all compliance training
- Overseeing the acceptable use of information and IT resources within their teams.
- Ensuring no new software systems or tools are procured by teams without consultation with IT Services
- Communicating starters and leavers within a timely manner
- Returning IT equipment when a person leaves.

6. ALL USER COMPLIANCE

6.1 To comply with these Regulations an authorised user of a University IT Resource shall:

a) Comply with applicable legislation and case law.

b) Comply with the Information Security Policy and other Regulations or Policies approved by the

University, and which are listed on the main University Policies and Procedures web site.

c) Adhere to the terms and conditions of all license agreements relating to University IT Resources which they use including software, equipment, services, documentation and other goods. This specifically includes the use of online library learning resources, including datasets, databases, e-books and e-journals which are subscribed to by the University. These are protected by copyright and license agreements. Users who are not covered by these license agreements will be blocked from accessing these resources.

d) When processing personal data ensure full compliance with all obligations under Data Protection Legislation. The University maintains information under the current legislation that should cover most data used for administrative purposes, but users are responsible for ensuring that any particular use of personal data complies with the University's Data Protection Policy and the data protection legislation. In cases of doubt, advice should be sought from the University's Data Protection Officer.

e) Use University approved systems, such as OneDrive or SharePoint to store work and data. Under no circumstances should confidential or sensitive data be stored on portable drives or personal online storage areas. For further guidance refer to the Information Classification and Handling policy .

f) Exercise due care and consideration for the interests of the University and other users, including the efficient use of consumables and other resources. In particular, they shall not engage in activities with the following characteristics:

- Misuse of IT Resources;
- Corrupting or destroying other users' data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using the network in any way which denies service to other users;
- Continuing to use an item of software or hardware after receiving a request to cease from the Authorised Personnel.
- Wasting support staff effort.
- Any activity infringing or being capable of infringing the Data Protection Legislation and all subsequent legislation.
- Any activity infringing or being capable of infringing the Counter-Terrorism and Security Act 2015 and all subsequent legislation

g) Users are expected to take all necessary precautions to prevent the spread of malicious software, such as viruses, malware, and ransomware. This means that:

- All files obtained from the Internet or external sources should be scanned for viruses and other malicious software before being used. Users must not circumvent University security systems.
- Software should only be installed from approved software centres. Installing software downloaded from the Internet or purchasing it independently is not permitted without prior approval from IT Services.
- Suspicious emails should be deleted immediately once identified. Emails containing unknown attachments or links should not be clicked on, and any email that appears unusual or unexpected should be handled with caution.
- If users have any concerns about the security of an executable file or suspect that a file may be malicious, it is their responsibility to immediately contact the IT Service Desk

for guidance before taking any action.

h) IT hardware must be treated with care and used only in accordance with the proper operating instructions. No equipment shall be used which is labelled “out of order”. Any apparent hardware faults should be reported promptly to the IT Service Desk. Equipment must not be used if there is reason to believe it is in an unsafe condition.

i) IT hardware or other Resources that are lost or stolen must be reported immediately to Line Managers and to the IT Service Desk.

6.2 No person, whether knowingly or negligently, shall:

a) Use another’s Username and Password to access an IT Resource.

b) Allow another person to use any Username issued to them to access an IT Resource.

c) Log in to an IT Resource and then leave the IT Resource unattended and usable by some other person.

d) Reveal their Password to any person. No-one, including members of IT, will ever ask an individual to reveal their account Password. Unauthorised use of your account is to be reported immediately to the IT Service Desk.

e) Distribute to a third party any software, the whole or any part of which, is subject to copyright without the express written permission of the copyright owner.

f) Attempt to decompile or otherwise reverse-engineer software without the written permission of the copyright owner.

g) Create, access, download, store, process or transmit any indecent, obscene, pornographic, racist images, data or other material, or any data capable of being resolved into such images, data or other material. An Authorised User may make a written request to the properly recognised authority for permission to have this clause of the regulations waived for properly supervised and lawful research purposes and in accordance with legal access permitted under the appropriate legislation. A written request must be made and written confirmation received in every case before any of the above acts are undertaken.

h) Create, access, download, store, process or transmit any terrorist related or extremist material, or any data capable of being resolved into such material (other than in the course of properly supervised, lawful and authorised research). This is a requirement of the University’s Prevent Duty under s26(1) of the Counter-Terrorism and Security Act 2015 as specified by guidance issued under s29(1) of the Act.

i) Create, access, download, store, process or transmit any defamatory material.

j) Create, access, download, store, process or transmit material that infringes the intellectual property rights of another person or organisation.

k) Create, access, download or store, process or transmit unsolicited commercial or advertising material.

l) Facilitate, encourage or allow deliberate unauthorised access to Resources or services accessible via thenetwork.

6.3 University provided IT resources such as computers, laptops, tablets, smartphones, and associated licensed software may not be reallocated without the prior approval of the properly recognised authority. Similarly, network storage allocations may neither be used by individuals or groups nor transferred to users other than those to whom they were originally given.

6.4 All requests to reallocate such resources must be submitted via the IT Service Desk and it will be a breach of these Regulations to relocate such resources without seeking and receiving this approval.

7. PERSONAL USE OF UNIVERSITY RESOURCES

7.1 Staff members are permitted to use electronic communications and information services for personal purposes subject to the following conditions:

- Such use should normally be outside their normal working hours.
- Use of email for personal external communications or for external registration for services should be limited and staff are advised not to use University email accounts and are reminded that access to these accounts will generally end if they leave the University.
- Staff must not use personal email accounts for University business and should avoid forwarding University-related information to personal email accounts.
- University communications and information Resources may not be used for personal financial gain, commercial ventures, or on behalf of external organisations unrelated to the User's professional activities.
- If members of staff are in any doubt about what constitutes acceptable and appropriate use they should seek advice from their Line Manager.

7.2 Access to the Internet should be managed in line with the terms of the Social Media Policy for staff. The Policy sets out how members of the University can use social media to promote the University and also expectations relating to responsible use of social media and the Internet for personal use during working hours.

7.3 Requests for electronic signature of documents (DocuSign etc.) must be forwarded to the appropriate signatory for the amount being agreed and any terms and conditions must be verified by Procurement or a Solicitor prior to final signature. Subscriptions to newsgroups and mailing lists are only permitted when the subscription is for a work-related purpose.

7.4 Students are permitted to use electronic communications and information services for personal purposes subject to the following conditions:

- University communications and information Resources may not be used for personal financial gain, commercial ventures, or on behalf of external organisations unrelated to their professional activities.

- If students are in any doubt about what constitutes acceptable and appropriate use they should seek advice from IT Services.

8. USE OF MOBILE TECHNOLOGIES

8.1 The use of personally owned devices such as PCs, laptops, netbooks, tablets, and smartphones, commonly known as BYOD (Bring Your Own Device), bring many benefits to the University: however, they pose a high-security risk if they are compromised, lost, or stolen. These risks must be recognised and addressed to protect both the physical device and the information they contain.

8.2 The University is committed to implementing effective measures to safeguard the use of mobile computing, communication, and storage devices. All employees of the University of Worcester and its subsidiaries who use mobile devices—such as laptops, tablets, smartphones, and USB drives—to access UW resources in public spaces, meeting rooms, or other unsecured areas, both on and off campus, are required to adhere to this policy and all other relevant documentation.

8.3 The following security controls must be activated on all devices when available to protect against the theft and damage of university data and systems. Users must:

- Control access to the device by setting a pin number, password, or biometric scan of sufficient length and complexity for the device type.
- Set the device to auto-lock after a period of inactivity of no more than 5 minutes.
- Install only licensed software from reputable sources and keep it up to date.
- Protect against malware by using anti-virus software and keep it up to date.
- Encrypt the device or the data stored on it if the function is supported by the device.
- Set up remote wipe facilities if available and implement a remote wipe if the device is lost or stolen.
- Never store sensitive or personal/confidential information on their personal devices as defined in the Information Classification and Handling Policy.
- Not attempt to circumvent the device manufacturer's security mechanisms. E.g., “jailbreak” an Apple device or “root” an Android device.

8.4 When travelling:

- Devices should be always kept in your possession.
- Avoid placing them in checked baggage and stay vigilant to the risk of theft, particularly at airport security checkpoints.
- When using a laptop, smartphone, tablet, or any other mobile device, avoid processing personal or sensitive data in public spaces such as airport lounges, public transport, or cafes.
- Be aware that public Wi-Fi networks are inherently insecure, and using them to handle sensitive information can put your data at risk.
- Passwords for UW systems should never be stored on mobile devices, as this could lead to theft or unauthorised access to information assets.
- Regularly back up your data before travelling so you don't lose important information if your device is lost or compromised.

8.5 If your device is lost or stolen, report it immediately to the IT Service Desk on 01905 857500 and notify your Line Manager.

9. COMMERCIAL USAGE

9.1 Unless otherwise expressly indicated, the University IT Resources and software supplied by or through the University are for educational or organisational use only. If any work is to involve commercial usage this should be reported to the IT Service Desk in the first instance.

9.2 Commercial usage of software supplied under “educational use only” agreements is permitted only if explicit written approval has been obtained from the supplier of the software, and consequentially, without such express authorisation, such use will be a misuse under the terms of these Regulations.

9.3 Any software, process or other invention developed by a member of the University using University IT Resources must not be commercially exploited without the prior consent of the University. For further guidance please refer to the UW Intellectual Property Policy.

10. GRANTS & EXTERNAL FUNDING

10.1 All requests to procure IT resources using research grants or external funding must be reviewed with the IT Service. This ensures compatibility with University systems and adherence to cyber security standards.

11. MONITORING

11.1 IT Services reserves the right to quarantine or completely remove a computer or device from the network where its configuration, operation or current status is shown to present a clear threat to the University. Examples would include a computer or device behaving in a way consistent with a virus infection. This may in extreme situations extend to quarantine a portion of the network in which the infected machine resides.

11.2 The IT team monitor accounts centrally for signs of misuse. If misuse of a University account is suspected the account may be accessed and/or disabled by IT without notice. IT will notify relevant staff of such misuse, which may lead to disciplinary action, and/or in the case of suspected criminal activity referral to the Police.

11.3 The University reserves the right to access, retrieve, intercept or delete any e-mail sent or received using the @worc.ac.uk address, as well as any other correspondence made using University managed hardware or software (Teams chats, posts and messages, phone calls, text messages, chats on messaging apps etc.). The purposes for doing so include but are not limited to:

- Statutory or business critical record keeping
- Ensuring compliance with regulations
- Preventing or detecting crime
- Investigating or detecting unauthorised use
- Virus checking or detection of other threats to University IT systems
- Responding to requests for information under Freedom of Information Act 2000 or the Environmental Information Regulations 2004, or a Subject Access Request under the UK GDPR
- Responding to an external request for information (e.g. from the Police or the Courts)
- Conducting a disciplinary investigation

Appendix 1

12. Definitions

The following expressions are used throughout this document, with the meanings assigned below:

a. “**The University Executive Board**” for example: the Vice Chancellor and Chief Executive, Director of Human Resources or Chief Information Officer (CIO).

b. “**Authorised user**” means a user who is registered with the University to use an IT Resource or set of Resources for a particular purpose or purposes; the term “**authorised use**” shall be interpreted accordingly.

c. “**Counter-Terrorism and Security Act**” means the Counter-Terrorism and Security Act 2015 and all subsequent related legislation.

d. “**Data Protection Legislation**” means the Data Protection Act 2018, and 'the UK General Data Protection Regulation (UK GDPR) and all subsequent related legislation.

e. “**IT Services**” includes all hardware, software, network/Internet access, printing and computer accounts and telecommunications.

f. “**IT Resources**” (or “**Resources**”) include personal computers whether desktop or portable, workstations, servers, tablets and mobile phones, computer peripherals, networks, data communication lines and equipment, telephone lines and equipment used for data communications, computer software and information stored in computer systems, and all databases and other computer-based information systems including all cloud based services hosted by3rd parties.

g. “**IT**” is the University’s Information Technology department, responsible for IT Resources.

h. “**Members of the University**” includes all members of staff, including affiliates, and all students.

i. **“Misuse**” of an IT Resource is any use of that Resource which constitutes a breach of these regulations or of any additional rules for the use of that Resource laid down by the appropriate properly recognisedauthority.

j. “**Password**” means the secret string of characters allocated to, or chosen by a user, that is used to gain access to University IT Resources. More information on setting passwords is available via the IT webpage

k. “**Prevent Duty**” means the University’s obligations under the Counter-Terrorism and Security Act 2015.

l. “**Publicly available data**” means all information made available via University IT Resources both to Members of the University and to external users by means of a public network such as the Internet.

m. “**Transmit**” means to transfer any form of data over the University’s data network or over any other network that is accessible from the University’s network.

n. “**University IT Resources**” includes all the resources that are owned, hired by, outsourced to or otherwise possessed or controlled by the University. The expression also includes all the resources that are provided for the use of Members of the University by other organisations as a result of a contract or other arrangement with the University or to personal equipment connected to the University network.

o. “**User**” means any person using or attempting to use University IT Resources, whether authorised or not, and the word “**use**” shall be interpreted accordingly.

p. “**User name**” means the identification given as part of the authorisation procedure that allows an authorised user to access a particular Resource. Normally a password is used with the user name to provide secure access to a Resource.

q. “**UW**” is the acronym used to indicate the University of Worcester.