01

Regulations for the use of IT Services and Resources

Index

Reference code	IT Regs v2.7
Author/originator	Deputy Director of IT
Approving Body	University Executive Board (UEB)
	28 –07 - 2021
Next Review Date	28 – 07 - 2024
Ratified/authorised by	Director of IT
Postholder/s responsible for review	Deputy Director of IT

Definitions

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

a. "**Authorised Personnel**" for example: the Vice Chancellor and Chief Executive, Director of Finance and Resources, and Head of Information Assurance. The IT Service Desk will maintain a list of authorised staff.
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 1998, and General Data Protection Regulation (GDPR) and all subsequent related legislation.
e. "**IT Services**" includes all hardware, software, network/Internet access, printing and computer accounts and telecommunications Resources provided by the University.
f. "**IT Resources**" (or "**Resources**") include personal computers whether desktop or portable, workstations, servers, mini and mainframe computers, 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 by 3rd 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 associate staff, 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 recognised authority.
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 or the World Wide Web.
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 natural or legal 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.

1. SCOPE

1.1 The regulations detailed in this document apply to anyone using IT Resources for any purpose at the University, including staff (temporary and permanent), students and visitors. *This includes personally owned equipment connected to the University's network from an external location, or on UW premises.*

1.2 These Regulations should be read in conjunction with the University's Information Security Policy.

1.3 The University provides access to external services including Internet access via the Joint Academic Network (JANET). JANET is the name given both to an electronic communications network and a collection of electronic communications networking services and Resources that support the requirements of the UK higher and further education and research community. The University may only take advantage of the benefits of this access through clear adherence to the Acceptable Use Policy specified nationally for all JANET users.

1.4 It is the responsibility of all authorised users of UW IT Resources to ensure that these Resources are 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. 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.

1.5 The University takes a strict approach to breaches of these regulations, which will be dealt with in accordance with UW'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 an authorised user (or any user) may suffer from any failure or malfunction of the University IT Resources or any parts thereof.

3. USER RESPONSIBILITIES

3.1 IT Resources are provided for the purpose of teaching, research, education and associated support.

3.2 Members of the University may use a University IT Resource provided that they are authorised users.

3.3 Authorised use will also be provided to anyone working with or at the University, subject to the discretion of Authorised Personnel. This may include, for instance, staff from other HE organisations or from professional bodies.

3.4 Possession of an account is a privilege which may be revoked at any time at the discretion of the Authorised Personnel.

3.5 The University IT Resources are provided for the academic work and normal University duties of Members of the University.

3.6 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 licence 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 academic purposes, but users are responsible for ensuring that any particular use of personal data complies with The Data Protection Act 2018 and any other relevant legislation. In cases of doubt, advice should be sought from the University's Data Protection Officer.

e) Have primary responsibility for the security and back-up of their work and data.

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;
- Wasting IT resources, including wasting time on an IT Resource;
- 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 reasonable steps to avoid the spread of malicious software, e.g. viruses. All files and software downloaded from the Internet or brought from home must be virus-checked before use. Suspicious emails should be deleted immediately upon receipt without being opened. If you are concerned about the security of any executable file please contact the IT Service Desk for advice.

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.

3.7 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 to IT immediately by calling the IT Service Desk on extension 7500.

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 the network.

3.8 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.

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

4. PERSONAL USE OF UNIVERSITY RESOURCES

4.1 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.
- Incoming personal phone calls during working hours should be limited to emergencies, as personal calls limit the number of external lines available for University business.
- No-one may use their @worc.ac.uk address in personal external communications or for external registration for services. This address must only be used externally for work-related purposes. Staff are advised to set up a private email address (e.g. Hotmail or Gmail) for external personal use. Staff should not use these 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.

4.2 Access to the Internet should be managed in line with the terms of the Responsible Use of Social Media Policy. 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.

4.3 Users must not commit UW to any form of contract through the Internet. 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.

4.4 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 the IT Services Department.

5. USE OF MOBILE TECHNOLOGIES

5.1 Mobile computing, communication and storage devices have become popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognised and addressed to protect both the physical devices and the information they contain. Special security considerations that relate to mobile devices include the following:

- Any malware (viruses, worms, Trojans) that infect the device can bypass the University's security and spread further into the network;

- If data stored on a mobile device is not backed up by the user it could be completely lost if the device is stolen or fails;
- Any sensitive data stored on a mobile device would be compromised should it be stolen or lost.

5.2 The University aims to ensure that effective measures are in place to protect the use of mobile computing, communication and storage devices. All UW employees using mobile computing devices (laptops, tablets, etc.), mobile communication devices (mobile phones, smart phones etc.) and mobile storage devices (USB memory sticks, CD/DVD's, etc.) to access UW resources in public places, meeting rooms, and other unprotected areas both within and outside the University of Worcester campus are expected to comply with this aspect of the Policy. This applies equally to information stored on or accessed via home PCs, laptops, tablets, etc.

5.3 Mobile Computing devices used by contractors, or third parties, to access the UW network, applications, and/or data are subject to the IT Regulations and Information Handling Guidelines.

5.4 The following security controls, when available, must be activated on all devices to help protect against theft of sensitive UW information contained on the device:

- Where sensitive information is held on laptops or mobile storage devices, data encryption must be applied to the information or to the entire device. Advice regarding encryption is available via the IT Service Desk.
- All mobile devices must have a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 15 minutes. 1 to 2 minutes is the recommended time.
- When not at your desk for an extended period of time your device must be physically secured (i.e. locked in a desk drawer or filing cabinet, locked in an office, or taken with you).

5.5 When travelling:

- Devices should be kept in your possession at all times.
- Do not put devices in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
- When using a laptop, do not process personal or sensitive data in public places e.g. public transport, cafe etc.
- Passwords for UW systems should never be stored on mobile devices where they may be stolen or permit unauthorised access to information assets.

5.6 If your mobile device, or UW sensitive information, is stolen or lost, you must report the loss as quickly as possible to your Line Manager and the IT Service Desk immediately.

5.7 If you transport or carry UW restricted data, or data that is classed as "special" under the data protection legislation on any mobile or storage device, be that a laptop, tablet, smartphone, USB data drive, or CD/DVD disc or similar, then that device must be encrypted.

5.8 It is recommended that any mobile or storage device containing UW confidential information that is only used within the University is also encrypted and/or locked away when the office is left unattended in case of theft.

5.9 Encryption software licencing, and guidance on how to encrypt a mobile device, is available from the IT Service Desk on extension 7500 or via the Service Desk Customer Portal. Staff considering

encryption of their personal computers should be aware that there are pitfalls, including the potential loss of access to data should they forget the master password.

6. COMMERCIAL USAGE

6.1 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.

6.2 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.

6.3 Where IT Resources are to be used in connection with research grants, short courses or contracts involving specific provision for computing costs, this fact must be communicated to the IT Service Desk.

6.4 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.

7. SECURITY OF PAYMENT CARD AND PAYMENT DATA

7.1 The University uses a variety of systems to process payments to and from members of the University and external individuals and agencies. This payment data, which includes sensitive information such as payment card data (e.g. PAN, CVV2) is maintained in line with Information Security Policy, the Data Protection Policy and data protection legislation. The following statements therefore apply specifically to payment card and payment data.

7.2 Payment card data will not be stored in electronic format, whether in local files, on spreadsheets or within databases.

7.3 Payment card data will not be shared by email under any circumstances, either internally or externally.

7.4 Payment card data or other payment data will not be removed from University premises.

7.5 In line with the Record and Document Retention Schedule, payment card and payment data will be retained for 12 months in paper format in a secure environment within the Finance Department, and no card detail will be kept electronically. In addition, access control log data or CCTV footage monitoring access to stored card data will be retained for 9 weeks.

8. MONITORING

8.1 The IT Service 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.

8.2 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. IT will initiate a *Compromised Account Procedure* in conjunction with the University's HR department when a University account is suspected of being misused.

8.3 The University reserves the right to intercept any e-mail sent or received using the @worc.ac.uk address and will monitor network traffic, including the Internet, for any of the following reasons:

- Record keeping purposes
- Checking compliance with regulations
- Quality control and staff training
- Preventing or detecting crime
- Investigating or detecting unauthorised use
- Virus checking or detection of other threats to University IT systems

8.4 In addition, Authorised Personnel may intercept and read messages if they are wrongly addressed.

8.5 Telephone numbers of calls to and from UW extensions are logged but the content is not monitored.