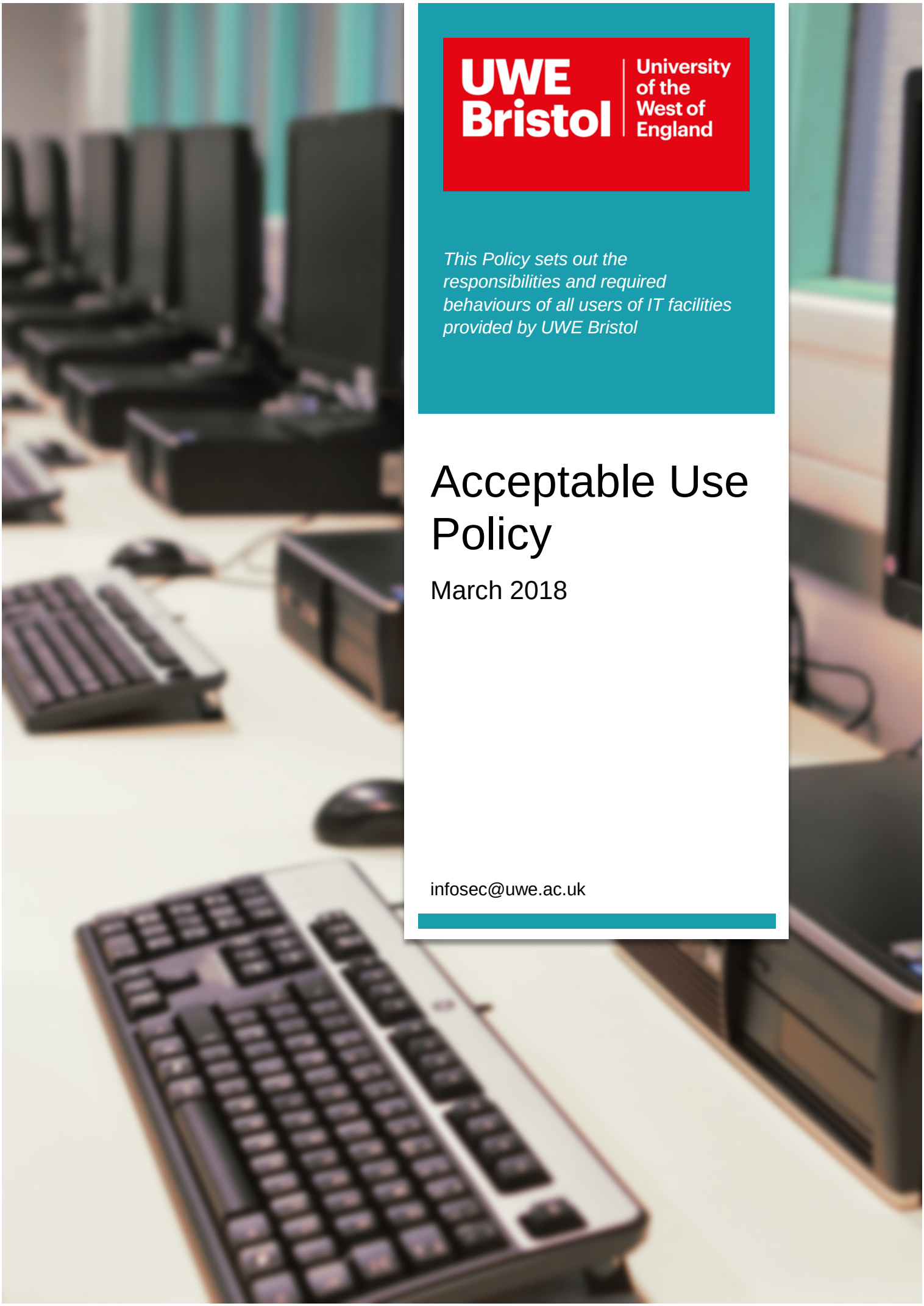

UWE Bristol | University of the West of England

This Policy sets out the responsibilities and required behaviours of all users of IT facilities provided by UWE Bristol

Acceptable Use Policy

March 2018

infosec@uwe.ac.uk

Contents

1. Purpose

The purpose of this policy is to explain the responsibilities staff, students and authorised third parties have in relation to their use of all electronic communications facilities, equipment and services provided by UWE Bristol.

It forms part of the Information Security Policy Toolkit, and underpins the overarching Information Security Policy. This policy provides everyone with guidance so they have clear understanding of the requirements that UWE Bristol places on them and the standards of behaviour expected.

2. Scope

The policy applies to all students and staff of UWE Bristol and all other third party users authorised by the University or any department thereof. It relates to the use of all electronic communications facilities owned, leased, hired or otherwise provided by UWE Bristol, connected directly or remotely to University infrastructure or used on University premises.

3. Responsibility

It is the responsibility of all students, staff and authorised third parties to ensure that their behaviour and activities when using UWE Bristol facilities is in accordance with the requirements of this policy.

4. Consequences of Policy Violation

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply may lead to the immediate cancellation of a contract. Where appropriate, breaches of the law will be reported to the authorities.

5. User Accounts

Those authorised to use UWE Bristol IT facilities are assigned an account for their individual use, under the following conditions:

- This account may not be used by anyone other than the individual to whom it has been issued
- The assigned account password must be changed immediately and not divulged to anyone, including ITS staff, for any reason
- For security reasons, this password must not be used as the password for any other account
- Individuals must remember their password and change it if there is any suspicion that it may have been compromised
- Individuals will also be assigned an individual email address for their use and some users may also be given authorisation to use one or more generic (role based) email addresses
- Individual email addresses are for the sole use of the assignee, but remain UWE Bristol assets and their use is subject to University policies

6. Equipment

The following statements define restrictions around use of personal and UWE Bristol provided equipment when using University networks or information.

- Equipment not provided and managed by ITS must not be connected to UWE Bristol internal networks (through network ports or staff only Wi-Fi) without the prior agreement of ITS
- Equipment on campus that is connected to the UWE Bristol network or otherwise managed by ITS may not be relocated without the prior agreement of ITS
- Staff and students are responsible for ensuring that all devices used in connection with university activity are password protected to safeguard any information held in the event of loss or theft
- Computers and other equipment used to access UWE Bristol facilities must be locked if left unattended while logged in
- Staff must ensure that they have up-to-date Anti-Virus software installed plus a firewall running at all times on equipment connected to the UWE Bristol network, including equipment not owned by or supplied by the University
- Any device that is not compliant with the above criteria is liable to physical or logical disconnection from the network without notice
- Serious damage or the theft of electronic communications equipment should be reported to the relevant campus security office which will advise the University Insurance Officer and ITS

7. Personal Use of UWE Facilities

UWE Bristol provides IT facilities, including email addresses and computers, for academic and administrative purposes related to work or study. Reasonable personal use is however permitted under the following conditions:

- it is used in a manner which does not obstruct the work of other students or staff and which encourages a scholarly atmosphere to be maintained
- it does not breach or undermine any UWE Bristol policies or codes of conduct
- it is not excessive in its use of resources

Members of staff and students should use only their UWE-provided email account when conducting University business. UWE Bristol computing facilities must not be used for the storage of data unrelated to the business or functions of the University. In particular, these facilities should not be used to store or share copies of personal photographs, media or personal emails.

8. Use of Third Party IT Services

Wherever possible, users should always attempt to use only IT services provided or endorsed by UWE Bristol for conducting university business. However, if a requirement arises that is not met by existing solutions, discuss this with the Head of Information Security in the first instance. An alternative solution may already be available or it may, subject to regulatory and procedural requirements, be possible to make use of services provided by third parties. Further information is available in the Information Handling Policy.

9. Unacceptable Use of UWE Facilities

Whilst not exhaustive, the following activities are considered to be unacceptable uses of UWE Bristol facilities. These restrictions are consistent with the JANET acceptable use policy (by which the University is bound) and the law.

- Any illegal activity or activity which knowingly breaches any UWE Bristol policy

- Any attempt to knowingly gain unauthorised access to facilities or information
- Any attempt to knowingly undermine the security or integrity of UWE Bristol facilities (including any unauthorised penetration testing or vulnerability scanning of any university systems)
- Providing access to facilities or information to those who are not entitled to access
- Any irresponsible or reckless handling or unauthorised use or modification of UWE Bristol data (see the Information Handling Policy)
- Any use of UWE Bristol facilities to bully, harass, intimidate or otherwise cause alarm or distress to others
- Sending unsolicited and unauthorised bulk email (spam)
- Creating, storing or transmitting any material which infringes copyright
- Creating, storing, accessing or transmitting defamatory or obscene material. (In the unlikely event that there is a genuine academic need to access obscene material, ITS must be made aware of this in advance and prior permission to access must be obtained from the Executive Dean)
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements
- Using UWE Bristol facilities for commercial gain without the explicit authorisation of the appropriate authority
- Failing to comply with a request from a member of ITS to desist from any activity which has been deemed by ITS to be detrimental to the operation of UWE Bristol facilities
- Knowingly failing to report any breach or suspected breach of information security to ITS (further information on incident reporting is available in the Information Security Policy)
- Failing to comply with a request from a member of ITS for you to change your password

10. Compliance with Legislation

In addition to the above requirements, UWE Bristol has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Individuals must also be aware of their responsibilities under the regulations listed below, and understand the fact that any infringement may result in action taken against them in accordance with University procedures:

- Counter Terrorism and Security Act 2015
- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Wireless Telegraphy Act 2006

10.1 GDPR

Failure to comply with data protection means the University is breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the University's reputation with the

media and other key stakeholders such as prospective students. Deliberate misuse of personal data is also a criminal offence for which you can be personally liable.

Personal data is any information attributable to an identifiable individual, including names and email addresses. For example, details of a student's academic performance and qualifications constitute personal data.

Sensitive personal data ("special categories" under GDPR) includes disability status, ethnicity, medical information (both physical and mental) and details of criminal convictions, and may require heightened security measures such as encryption and stricter access controls.

11. Monitoring

Monitoring of individual usage of the electronic communications facilities will not be undertaken as a matter of course. However, this may be necessary when concerns arise about the level or nature of personal use of the systems. Disciplinary action may be considered appropriate in such circumstances. Further information is available in the Information Security Policy.