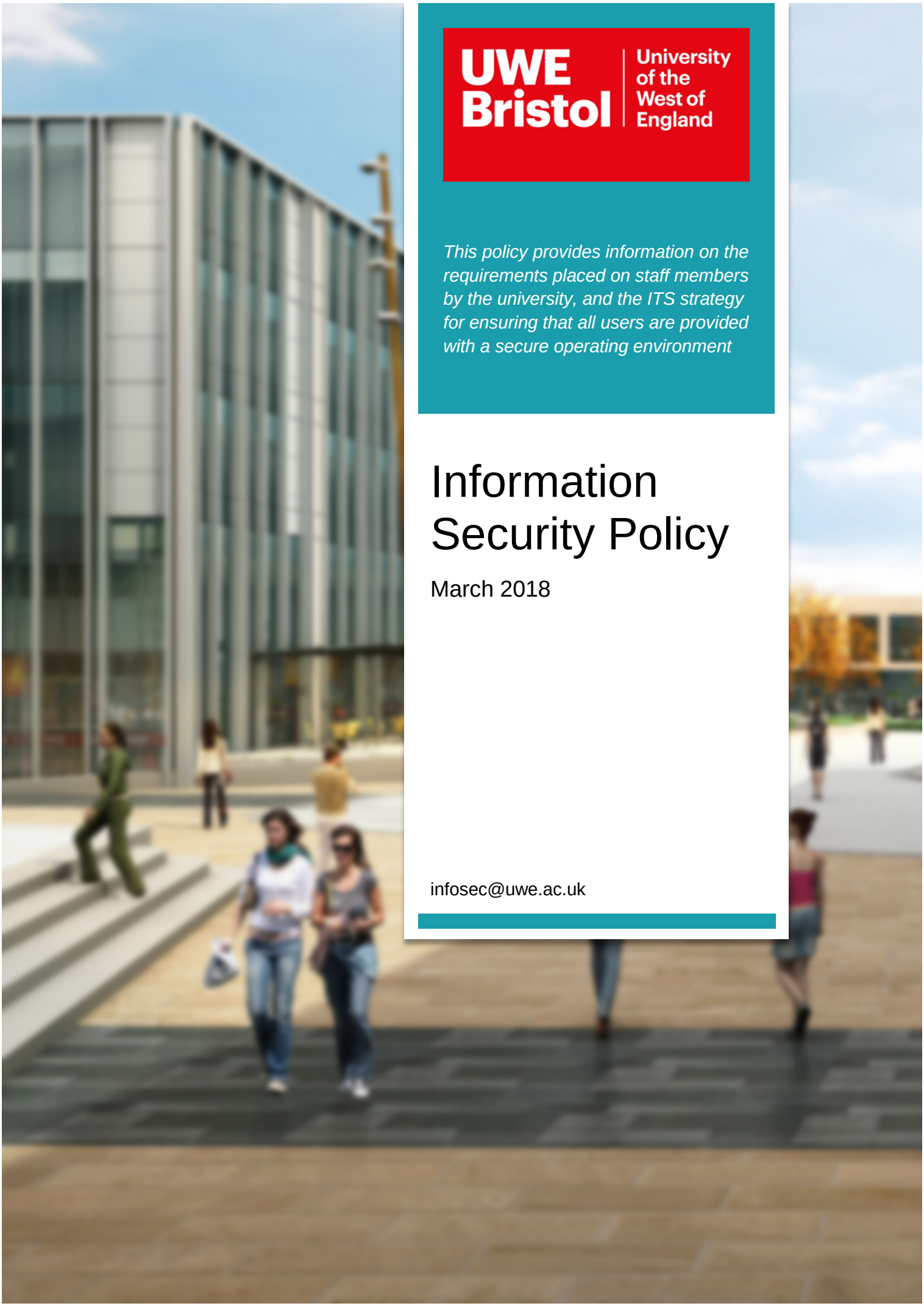

UWE Bristol | University of the West of England

This policy provides information on the requirements placed on staff members by the university, and the ITS strategy for ensuring that all users are provided with a secure operating environment

Information Security Policy

March 2018

infosec@uwe.ac.uk

Contents

1. Purpose

This policy ensures that all technology and information assets provided and managed by UWE Bristol are adequately protected against security threats including compromise, loss, unauthorised disclosure and other misuse.

It provides guidance to everyone who use UWE Bristol IT facilities to ensure they are aware of, and able to comply with, the requirements placed upon them by all associated Information Security policies, and are also aware of and able to work in accordance with the relevant procedures, legislation, and codes of practice.

2. Scope

The policy applies to all anyone authorised by UWE Bristol or any department thereof. It relates to the use of all UWE Bristol IT facilities; to all private systems (whether owned, leased, rented or on loan) when connected to the UWE Bristol Infrastructure; to all UWE Bristol owned or licensed data and technology; and to all data and technology provided to UWE Bristol by partners or external agencies. The policy also relates to paper files and records created or held by UWE Bristol.

3. Consequences of Policy Violation

A copy of this policy will be issued to all account holders upon activation of their user account. Existing students and staff of UWE Bristol, as well as authorised third parties with access to IT facilities will be advised of the existence of this policy and the availability of the associated policies, procedures, guidance and training. 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.

4. Education and Awareness

To ensure that students and staff are provided with the necessary information to allow them to make informed decisions on security, UWE Bristol is committed to providing training and guidance on security issues and best practice recommendations. Students and staff are entitled to training, and UWE Bristol reserves the right to mandate specific security training (e.g. information security module) as a criteria of continued access to provided IT facilities. Any such training will be introduced in line with UWE Bristol agreed processes.

5. Responsibility for Information Security

All users of UWE Bristol IT facilities have a personal responsibility to manage and protect information under their possession, and may be personally liable for any incidents that arise from a failure to take appropriate protective measures. Individuals also have a responsibility to act in a vigilant and professional manner, by refraining from any action that may jeopardise the integrity or security of UWE Bristol systems, and promptly reporting any suspected security violations. It is the responsibility of every student, staff and authorised third party to understand and act in

accordance with all Information Security policies and procedures instituted at a University-wide or departmental level.

Staff with line management responsibilities must ensure that their supervised staff members are aware of, and comply with, security best practices.

All Directors and Faculty Executives within the university are responsible for ensuring that Information Security policies are implemented and complied with across their respective areas. This includes promoting security awareness and best practices among staff, and maintaining full oversight over activities that have the potential to influence the confidentiality, integrity or availability of UWE Bristol information or infrastructure.

The Information Security Forum is responsible for the review and approval of all policies relating to Information Security at UWE Bristol. This is an ITS group comprised of management and technical representatives, and meets on a regular basis to review operational and strategic Information Security activities. As such, the Information Security Forum can also advise on matters related to compliance with these policies, and may introduce supplemental information, guidance or procedures with respect to these policies. The Information Security Forum is responsible for regularly assessing Information Security policies to ensure their usability and accuracy.

6. Legislative Compliance

Students and staff have an obligation to abide by all UK and relevant EU legislation. With respect to information security, of particular importance are the Computer Misuse Act 1990, the Data Protection Act 1998, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000.

6.1 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.

7. Monitoring

Monitoring of individual usage of the electronic communications facilities will not be undertaken as a matter of course. However, Many UWE Bristol systems maintain transaction and event logs, which record information about each transaction being carried out. The content of these records vary, but may contain the following information:

- the date and time of the transaction
- the number of bytes transferred in the transaction
- the unique source and destination IP address of data packets
- the type of process
- the Universal Resource Locator (URL)
- the login identity of the person making the transaction
- the source and destination address of E-mail transactions

These logs are essential to the efficient running of IT systems and are maintained by ITS operations staff for the following reasons: capacity planning; traffic and/or transaction flow monitoring; system monitoring; transaction tracking; fault diagnoses; system security; virus detection and auditing.

In cases of security breaches, system malfunctions, the receipt of substantiated complaints from other organisations and virus or hacking attacks, these logs may be used as part of an investigation to trace transactions through the system to a particular PC or individual.

Internet 'web caches' are used to improve the retrieval times of frequently accessed web pages and store a complete copy of accessed pages for a predetermined period of time. Caches of pages are maintained at various points within the system. In some circumstances, such as the detection of virus attacks or investigations into computer abuse, authorised personnel from ITS may search the content of web caches.

8. Information Security Policy Toolkit

This policy relates to, and is supplemented by, a number of policies that pertain to the confidentiality, integrity and availability of UWE Bristol information and technology assets. These policy documents form the Information Security Policy Toolkit, and a list of the supplementary policies is given below. Acceptance and compliance of this policy is contingent upon compliance with all policies provided in the Toolkit.

- Information Handling Policy
- Remote Access Policy
- Acceptable Use Policy

Each of the policies within the Toolkit contains high-level descriptions of requirements and principles. They are not intended to provide detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents, guidance articles, and supplementary information which will be made available in conjunction with the relevant policy document. Any substantive changes made to any of the policies within the Toolkit will be communicated to all relevant personnel.

9. Reporting Information Security Incidents

It is our responsibility to ensure we follow the correct steps to protect the security of staff and student data. We also need to report data protection breaches immediately. The following guide outlines the steps you must take to report any potential data security breaches straight away.

1. Report any potential breaches to the IT Service Desk by phone on +44 (0)117 32 83612 or dial 123 immediately. This is essential to control the risk to you, data subjects and the University.
2. For IT-related breaches (eg response to a phishing email or lost device) change your password. This will help ensure personal information is not compromised.
3. If the suspected data breach concerns lost or found physical information (e.g. a box of paper records) or a mobile device, contact the Security Office. Security will also report the breach to IT Services on your behalf.