UWE Bristol | University of the West of England

This policy provides controls regarding remote access to protect both individuals and UWE Bristol from accidental loss or disclosure of University information

Remote Access Policy

March 2018

infosec@uwe.ac.uk

Contents

1. Purpose....2
2. Scope....2
3. Responsibility....2
4. Consequences of Policy Violation....2
5. Remote Access Principles....2
6. Remote Access Services....3
6.1. Staff Services....3
6.2. Student Services....3
6.3. Email....3
7. Information Risks....4
8. Processing of University Information on Private Devices....4
9. Device Security....4
10. Device Theft....5

1. Purpose

The increasing adoption of mobile working and remote access technologies allows students and staff to access UWE Bristol services and information from anywhere with an internet connection. This manner of working also increases the risk of data being accidentally or maliciously copied, modified, hidden, or destroyed. ITS provides solutions to minimise these risks to UWE Bristol information, however when using remote access services staff and students have a personal responsibility to ensure they understand and abide by secure working practices.

This document forms part of the Information Security Policy Toolkit, and underpins the overarching Information Security Policy. Adherence to this policy will minimise risk to information that is being compiled, used, transported or held outside UWE Bristol premises, where security protections may be lower and exposure to risk may be greater.

2. Scope

This Policy is directed at those who utilise either privately owned or UWE Bristol provided portable devices, such as laptops, tablet computers, and mobile phones to participate in mobile working. The policy also applies to those who access UWE Bristol systems from home or other remote locations using either privately owned, third-party-owned or University owned equipment.

3. Responsibility

It is the responsibility of UWE Bristol to ensure that appropriate technical facilities are available to enable compliance with the Remote Access Policy. It is the responsibility of all students, staff and administrators 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. Remote Access Principles

Portable devices that are used for mobile working, and home computers that are used to remotely access UWE Bristol information or services, must be managed effectively in order to minimise the risk that (1) sensitive or confidential information may be mishandled, lost or compromised and (2) staff using such devices may inadvertently fall foul of the law.

In some instances disclosure, corruption or loss of UWE Bristol information may result in minor disruption. However, in the case of research data or personal information the consequences are potentially very significant, and therefore more stringent conditions are placed upon access and storage. The unauthorised disclosure, modification or loss of this type of information could result in the prosecution of individuals for breach of the Data Protection Act 1998 if it was found that the data had not been protected and managed in accordance with the requirements of The Act.

Appropriate care and diligence must be taken to prevent or minimise the possibility of loss or theft of UWE Bristol provided computers. Mobile workers must be cognisant of the environment in

which they are working and apply appropriate common-sense measures to protect UWE Bristol provided computers and data. Working on confidential information should be avoided in public spaces e.g. coffee shops or trains, due to the possibility of unauthorised individuals viewing or overhearing this information.

5.1. 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.

6. Remote Access Services

The UWE External Access (XA) service allows both staff and students to gain access to their personal drive H: and faculty shared drives S: (and also T: for staff members) from private devices over the internet.

6.1. Staff Services

All staff members using XA have access to the UWE staff intranet which provides the same features as it does on campus. XA also provides a remote UWE desktop to allow users to access the same resources that they access from their University desktop/laptop whilst on campus. The connection provided is secure, with data traffic encrypted, and the data is saved on the respective user's 'H' drive instead of on the local hard drive of the machine being used for the access. In addition, staff can also access SharePoint, OneDrive, and Office365 externally through the web portals for these respective services.

6.2. Student Services

In addition to XA, students are able to remotely access myUWE, an online portal to services such as Blackboard, e-library and UWE Email, to access specific information not externally available.

6.3. Email

Alternatively, anyone who simply needs to access their email is able to use the University's Outlook Web Access facility, or remotely connect to their university email account from Outlook and other popular email clients. However, this service must not be used to download Confidential attachments to non-UWE provided devices. Further details regarding information classifications and sharing arrangements are available in the Information Handling Policy.

7. Information Risks

Information that is held or processed on systems outside of UWE Bristol Infrastructure is generally more exposed to being compromised, corrupted or lost than information that is held or processed on systems within the University. For example:

- Laptop computers may be stolen, lost or left on public transport
- When used in public, data displayed on laptop computers may be subjected to viewing by unauthorised persons
- Data can remain on mobile or remote systems after accessing UWE Bristol systems without some users being aware (such as cached web pages and e-mail attachments)
- UWE Bristol has no jurisdiction over privately owned equipment and when this has been used to access university information, this data may be available to be viewed by unauthorised persons
- The security of machines outside UWE Bristol premises, in terms of security patching and virus protection, may be lower than those within the University and exposure to hacking attacks and virus contamination may be higher
- Physical security in the home may be lower than that of UWE Bristol premises, and some domestic properties may be more prone to burglary resulting in the theft of laptops and private computers

8. Processing of University Information on Private Devices

In accordance with the Information Handling Policy, users must be aware that, unless using the XA service to do so, privately owned computers cannot be used for the creation, storage or processing of:

- ‘Restricted’ or ‘Confidential’ data as defined in the Information Handling Policy
- Data which is recognised as being of high importance, or where there is no up-to-date backup or copies stored elsewhere

It is essential that those participating in mobile and remote working practices familiarise themselves with their responsibilities under the UWE Bristol Information Handling Policy and Data Protection Policy.

All mobile and remote users are personally responsible for ensuring that any University data on their machines (UWE Bristol provided or otherwise) is regularly and frequently backed up and that backup media is handled and stored in accordance with the Information Handling Policy.

9. Device Security

Individuals are responsible for the safekeeping and protection of UWE Bristol provided IT equipment that has been issued or loaned to them. Anyone in possession of UWE Bristol provided portable devices are also responsible for ensuring unauthorised users do not gain access to them, and the devices themselves should not be transferred or loaned to anyone without prior approval from the issuing authority.

Anyone that accesses, produces or stores UWE Bristol information on privately owned computer equipment is responsible for the security of both the data and the device holding it. In order to protect UWE Bristol information, such machines must have adequate Anti-Virus protection, as

well as an active firewall and all available security and maintenance patches applied. As above, individuals are also responsible for ensuring against unauthorised access to the UWE Bristol information when using their computer.

Devices provided by UWE Bristol may be more appropriate where there is a significant requirement to access university data and resources in support of university business. These devices provide greater access to UWE resources (including personal drives). Appropriate support is available for them via ITS and the range of products is sufficient to suit the majority of University business needs.

10. Device Theft

1. The loss of any UWE Bristol provided device is a potential data breach therefore you must report this 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. 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.