Remote Access Policy

Version:	**3.0**
Dated:	**26 June 2020**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Author	Summary of Changes
1	Unknown	Exeter IT	Creation
2	18/4/19	Ali Mitchell	New template and changes to layout. Some new hyperlinks added and related policies section
2.1	16/9/19	Ali Mitchell	Added in reference to associates in numerous paragraphs; changed the use of data to information; added in locks screens to para 6.3 and up-to-date anti-virus software to para 10.4
2.2	24/3/20	Ali Mitchell	Changed reviewers. Removed section on Processing of Uni information on private devices as belongs in Acceptable use Policy
2.3	3/6/20	Ali Mitchell	Minor changes to Help and Advice section
2.4	26/6/20	Ali Mitchell	Added into para 3.2 cloud hosted software/applications/services/environments. 7.2 added MFA, IPsec SSL and HTTPS. Added in another paragraph 6.1; users should not download and store Uni information on personal devices. Previous para 6.1 now 6.2. Added in para 12, policy review and maintenance

Review Distribution

Name	Title
Mike Maling	Operations and Security Manager
Brenda Waterman	Information Governance Manager and DPO
Simon Hallett	Security Architect
Martyn Goldsborough	Information Security Manager
Ira Goel	IT Risk and Compliance Manager

Approval

Version	Members / Position	Date
1	Unknown	N/A
2	Update to existing policy template	N/A
2.1	IGSSG members	unknown
3	Members of ISG	1/7/2020

Contents

1. Introduction

1.1 The University of Exeter (UoE) recognises the importance of its staff, associates and students being able to work efficiently and remotely away from its campuses. However, it is important that remote IT users ensure they take care to work in a secure manner and not cause increased risk to the University's infrastructure and reputational concerns.

2. Purpose

2.1 The increasing adoption of mobile working and remote access technologies allows students, associates and staff to access University of Exeter services and information from anywhere with an internet connection. This manner of working also increases the risk of information being accidentally or maliciously copied, modified, hidden, or destroyed.

2.2 IT services provides solutions to minimise these risks to UoE information, however when using remote access services staff, associates and students have a personal responsibility to ensure they understand and abide by secure working practices.

2.3 This document forms part of the University's Information Security Strategy and underpins the Overarching Information Governance and Security Policy. Adherence to this policy will help minimise risk to information that is being compiled, used, transported or held outside UoE premises, where security protections may be lower and exposure to risk may be greater.

3. Scope

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

3.2 This policy applies to any University resources that can be accessed remotely, such as University supplied and supported office software packages. This would include Office 365 and applications such as Word, SharePoint, OneDrive for Business, Teams, and other cloud hosted software, applications, services and environments.

4. Responsibility

4.1 It is the responsibility of UoE to ensure that appropriate technical facilities are available to enable compliance with this Remote Access Policy.

4.2 It is the responsibility of all students, staff, associates and administrators to ensure that their behaviour and activities when using UoE facilities is in accordance with the requirements of this policy.

5. Policy Violation

5.1 Failure of an individual student, associate 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.

5.2 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.

6. Remote Access Principles

6.1 Non University supplied / home computers used for University work must not download and store official and / or sensitive files on these devices. Where this cannot be avoided, users must ensure they completely delete the files when no longer required.

6.2 Portable devices (including laptops, tablets, mobile telephones, PDAs etc.) that are used to remotely access UoE information or services, must be managed effectively to minimise the risk that:

- sensitive or confidential information may be mishandled, lost or compromised and
- staff and associates using such devices may inadvertently fall foul of the law

6.3 In some instances, disclosure, corruption or loss of UoE information may result in minor disruption. However, in the case of research material or personal information the consequences are potentially very significant, and therefore more stringent conditions are placed upon access and storage. Refer to the relevant supporting policies in paragraph 12.

6.4 Appropriate care and diligence must be taken to prevent or minimise the possibility of loss or theft of UoE provided computers. Mobile workers must be cognisant of the environment in which they are working and apply appropriate common-sense measures to protect UoE provided computers and information. For example, ensure screens are locked when moving away from a device (even for short periods). Working on confidential information must be avoided in public spaces e.g. coffee shops or trains, due to the possibility of unauthorised individuals viewing or overhearing this information.

6.5 When creating and storing documents in University resources such as SharePoint, Teams etc. users must ensure the appropriate labelling of documents and retention policies are set / applied

6.6 Users of SharePoint, OneDrive for Business, Teams etc. are required to complete the necessary training before starting to use these services. For example, SharePoint site owners must complete the training before a site is created. All users also have to undertake Information Governance Training every 2 years.

7. Remote Access Services

7.1 External access allows both staff, associates and students to gain access to their personal drive and shared drives from private devices over the internet.

7.2 Staff / Associates Services

- External access also allows users to access the same resources that they access from their University desktop/laptop whilst on campus via the Virtual Private Network (VPN). The connection provided is secure, ensuring information / data transfer is encrypted (such as using multi-factor authentication; IPsec, SSL and HTTPS). In addition, staff and associates can also access SharePoint, OneDrive, and Office365 externally through the web portals for those respective services.

7.3 Student Services

- Students can remotely access iExeter, an online portal to various services, such as student guidance, timetabling, and their library account.

7.4 Email

- Anyone who needs to access their email can connect to their university email account from either the Outlook Client or through the Office365 platform.

8. Information Risks

8.1 Information that is held or processed on systems outside of UoE 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, information displayed on laptop computers may be subjected to viewing by unauthorised persons.
- Information can remain on mobile or remote systems after accessing UoE systems without some users being aware (such as cached web pages and e-mail attachments).
- UoE has no jurisdiction over privately owned equipment and when this has been used to access university information, it could be available to be viewed by unauthorised people.
- The security of machines outside UoE 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 UoE premises, and some domestic properties may be more prone to burglary resulting in the theft of laptops and private computers.

9. Device Security

9.1 Individuals are responsible for the safekeeping and protection of University of Exeter provided IT equipment that has been issued or loaned to them.

9.2 Anyone in possession of University of Exeter 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.

9.3 Anyone that accesses, produces or stores University of Exeter information on privately owned computer equipment is responsible for protecting the information and the device holding it.

9.4 To protect University of Exeter information, such machines must have up-to-date anti-virus software, adequate anti-malware protection, as well as an active firewall and all available security and maintenance patches applied.

9.5 As above, individuals are also responsible for ensuring against unauthorised access to the University of Exeter information when using their computer. Devices provided by University of Exeter may be more appropriate where there is a significant requirement to access university information and resources in support of university business. These devices provide greater access to UoE resources (including personal drives). Appropriate support is available for them via the IT service and the range of products is sufficient to suit University business needs.

10. Device Theft

10.1 The loss of any University of Exeter provided device must be reported to SID as soon as is practical.

11. Supporting Policies and Documentation

11.1 This policy should be read in line with associated standards, policies and arrangements including:

Password Policy

Information Classification Policy

Records Management Policy

Information Retention Policy

Information Sharing Policy

IT Guidance for Homeworking

VPN and Network Guidance

Privacy and Personal Data Protection Policy

Bring Your Own Device Policy

Regulations Relating to the Use of Information Technology Facilities

Information Security Controls Policy

Information Security for Portable and Removable Media Devices Policy

12. Policy Review and Maintenance

12.1 This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

13. Help and Advice

13.1 Please contact either the Information Governance Team information-security@exeter.ac.uk or IT Security and Compliance itsecurityandcompliance@exeter.ac.uk