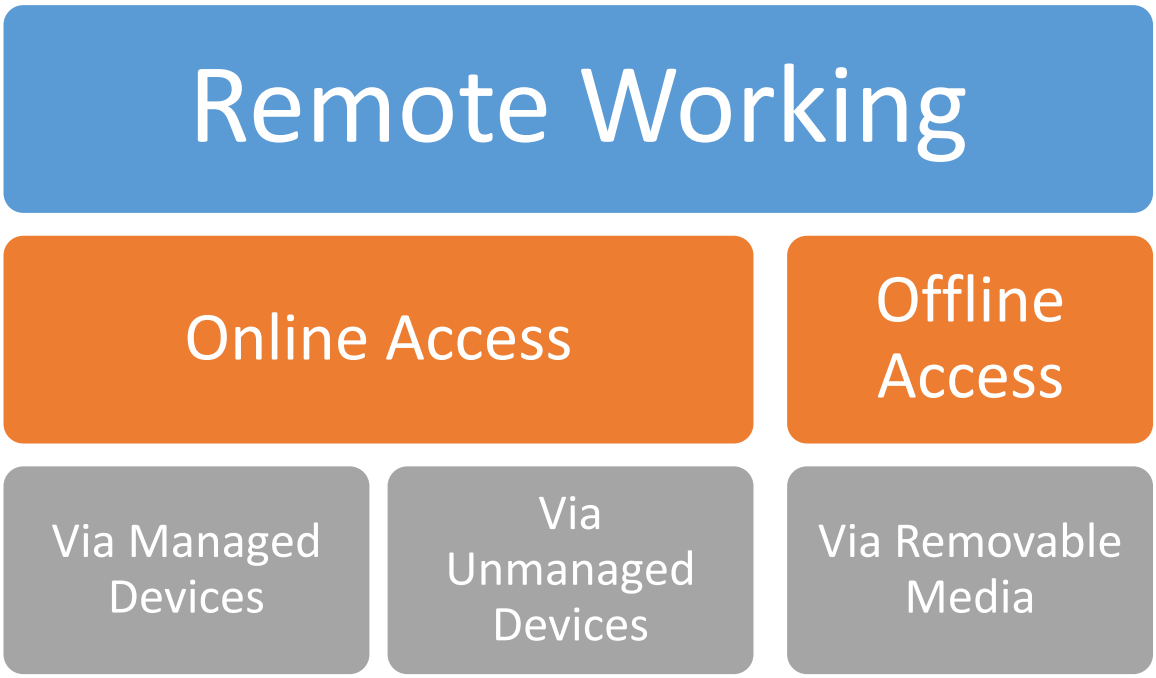
IT Remote Working Policy

1. Purpose

To ensure that all staff processing information remotely (i.e. not at a PC on campus) do so securely and in accordance with the Data Protection Act 1998.

This policy has been written to ensure that staff are aware of their individual responsibilities around information security when working remotely. It applies to all staff who use or access University systems or information remotely either occasionally or as part of their contract. It applies to information in all formats, including manual records and electronic data.

The diagram below shows the relationship between the differing means of working with University information off campus.



The differences between the three methods of remote working are described below:

1.1 Managed Device Overview

A managed device will be a laptop conforming to the University's Business Computing Standard (http://url.tees.ac.uk/bcs), utilising "Direct Access" technology, a tablet / phone utilising "ActiveSync" technology or an IronKey memory stick featuring remote management. These devices, warranted by the

IT Department's Information Assurance Team can be remotely managed, are encrypted and highly secure.

1.2 Unmanaged Device Overview

Typically, this will be a staff member accessing University resources from a home computer. Accessing University resources from third party computers (friends, internet cafés) is highly dangerous due to the lack of certainty over malware protection.

There are three modes of access from unmanaged devices:

- Remote Desktop Services (RDS): Formerly Citrix, this technology essentially mirrors a University based PC screen and keyboard to the local PC. The only data that needs to transfer between the local PC and the University are key-presses (to the University) and screen updates (to the local PC).

- Virtual Private Networks (VPN): For general staff VPN access has been superseded by "Direct Access" via a managed device. VPN access is now only available to specifically authorised University IT staff and third parties for the purposes of remote technical maintenance activities.

- Web: Logon via a local web browser to extranet resources such as Unity, Outlook Web Access etc. No access is permitted to purely internal corporate information systems (Finance etc.) from an unmanaged device other than via use of Remote Desktop Services (formerly Citrix).

It is the goal of the University that all access from unmanaged devices will utilise multi-factor authentication (MFA). MFA requires the remote user to not only have a valid staff id and password but also to have a physical object in their possession. Typically, this will be a mobile phone and part of the logon process will utilise that device to validate that the id and password are not stolen. Due to single-sign on capabilities, staff accessing multiple systems from the same web browser session should not have to log on for each individual system.

1.3 Removable Media Overview

Access via Managed and Unmanaged devices rely to some degree on off-campus internet access, though data already stored on a secured managed device can be worked on independently. The final and least secure method of manipulating corporate information remotely is to take a copy on a USB memory stick or other removable media. This should be used as a last resort as it is the most vulnerable to data loss and virus transmission. Encryption must be enabled unless the content is for open public consumption. Encryption of the device by default is the safest option, though some knowledge where it will be used is beneficial to ensure it can be decrypted as required. Unfortunately, there is no standard, built-in encryption tool that works across all computing platforms.

2. The Policy

The safest way to work on University information is to do so on campus via a device managed by the IT Department (local working). That device will be securely configured, regularly updated and connected to a secure network. All forms of remote working introduce an element of risk through either data loss or ingress of malware.

In consideration of the fact that remote working is often necessary or desirable for business reasons consideration has been given as to the methods of providing the capability whilst maintaining a high degree of safety. The table below summarises methods of accessing information and levels of security offered.

Technology	Managed Device	Unmanaged Device
1. Direct Access	**x**	
2. ActiveSync	**x**	
3. IronKey	**x**	
4. Remote Desktop Services (RDS)		**x**
5. Virtual Private Network		**x**
6. Web (extranet: Outlook, Unity, etc.)		**x**
7. Removable Media (Memory stick etc.)		**x**

Permission needs to be sought and recorded with regard to the use of Technologies 1-5. See Appendix A.

2.1 Remote Working via a Managed Device

The most secure and due to the reliance on equipment, the costliest form of remote working. Given that a managed device will hold and provide immediate access to corporate information the following must be borne in mind:

- Only managed devices provided and/or authorised by the IT Department are permitted.
- Managed devices provided by the University are formally recorded against individuals in the Assets system. They will be subject to audit and must be returned as part of the leavers process.
- Using the managed device for anything other than work purposes is potentially dangerous especially personal web-browsing.
- The managed device must not, under any circumstances, be allowed to be used by a third party (non-University employee). This includes family, friends etc.
- Any theft or loss of the device must be immediately reported to the IT Department and or the authorities. A police crime number will be required in the case of stolen assets.
- If there is any suspicion that you have disclosed your device password, it should be changed immediately.
- Encryption or any other aspects of the security configuration must not be disabled or altered.
- In the case of “Direct Access” all web traffic is routed via the University’s network and subject to normal logging and protection.
- The use of a Managed Device requires authorisation (See Appendix A).

2.2 Remote Working via Unmanaged Devices

Unmanaged devices are by definition outside of the University's control. Thus there can be no certainty that the machine is regularly updated, secure and uninfected with keyboard loggers or other malware. Individuals may have some sense of the state of the security of their home computer but do exercise great caution if it is a shared device (family etc.) as other family members may not be as diligent as yourself.

Please note the following requirements:

- A home PC used for remote working must have anti-virus software installed and up to date, have all operating system patches applied and be regularly scanned for malware.
- Refrain from copying University information (files etc.) to the hard disk of the home computer. They may be discovered by others or when the computer is disposed of. The University will assist staff members in safely disposing of home computers.
- Third party computers like those of friends or internet cafés must not be used to access University resources due to the malware risk.
- Never select any options to remember passwords or store logon credentials on the remote computer.
- Only remote access services provided by the IT Department (see table above) are permitted to be used.
- Staff are expressly forbidden from configuring any means of accessing their work computer remotely. E.g. TeamViewer, Chrome extensions, LogMeIn, GoToMyPC, VNC etc.
- Other than via "Direct Access" or "Remote Desktop Services" (see above table) it is not permitted to access the administration interfaces of corporate information systems. E.g. Finance, Payroll or SITS data.
- It is vital that any access service (4-6 in the table above) is logged off and web browsers closed upon completion of activities.
- Third party (system suppliers) access to University resources (for the purpose of maintenance) must be completely controlled:
    - Access must only be enabled when required and closed afterwards.
    - The purpose and intent of any work noted.
    - Due diligence undertaken with regard to how the third party will manage security credentials provided by the University.

2.3 Remote Working via Removable Media

The use of Removable Media (mainly memory sticks or USB drives) is a common form of remote working. However, it is the least secure by design as there is a high reliance on human beings to deliver the required levels of security.

There are high end/cost variants (e.g. IronKey memory sticks) which are highly secure, multi-platform and remotely manageable They are actually small internet aware computers and would be classified in this document under "Managed Devices" (See 2.1).

When using removable media, note the following:

- Highly Confidential information should never be stored on removable media (See Information Classification within the Information Security Policy http://url.tees.ac.uk/isp).
- All removable media must be encrypted, unless the content is for open public consumption.
- The only removable media formats permitted are memory sticks and USB drives. Any other media formats (DVDs etc.) must be cleared with the IT Department's Information Assurance Team to ensure that the media can be suitably encrypted.
- The IT Department can provides simple guidance on how to encrypt media via a device corresponding to the University's Business Computing Standard (http://url.tees.ac.uk/bcs). Any other form of encryption must be cleared with the IT Department's Information Assurance Team to ensure it is strong enough.
- Please be aware that when you plug removable media into a third party device, that device may infect the memory stick with malware.

2.5 Cessation

Remote working facilities will be terminated when a staff member leaves the institution. Should the need for remote working be removed at any other time, the IT Department must be informed.

Staff must return any equipment issued for remote working purposes when no longer required.

2.6 Breach

Individuals in breach of this policy are subject to disciplinary procedures (staff or student) at the instigation of the Dean/Director (or above) with responsibility for the relevant information system.

3. Ownership

3.1 The Director, IT and Communications Services (IT Department) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

A. Appendix: Remote Working Request Form

Requests for remote working are made by online form, which is available here: http://url.tees.ac.uk/forms. Please ensure you have read the policy before making an application.