Data Storage and Remote Working Policy

Version Control

Version	Date
Draft 0.2	05/10/2017
1.0	01/11/2017

Related Polices

- Information Services Acceptable Use Policy
- Associate Accounts Policy
- IT Security for 3rd Parties, Suppliers and Support Organisations Policy
- Access Control Policy

1. Introduction

1.1. Background

The ever increasing use of digital information at the University increases the risk of data being copied or stolen, or modified, hidden, encrypted or destroyed. Although technical controls provide an essential element of protection, it is essential that these are combined with good working practices and staff awareness of security risks.

Portable computers and devices that are used for mobile working, and home computers that are used to remotely access to University computing resources, have to be managed effectively in order to minimise the risk that certain information will be lost or compromised.

1.2. Purpose, Applicability and Scope

This Policy provides controls in respect of data storage and remote access to the University's information assets to protect both individuals and the University from the consequences of accidental disclosure or loss of such information. It is not intended to create an obstacle to mobile and remote working, and is not intended to support or advocate working from home.

This Policy addresses the need of the University to ensure that we:

- take responsible ownership or stewardship of all data
- follow legal, regulatory and compliance needs
- ensure the confidentiality of data
- ensure the integrity of data
- ensure the availability of data (data is accessible whenever it is required).

This Policy is primarily directed at:

- Staff and students who use either privately owned or University owned portable computers, such as laptop and tablet computers, and mobile phones with computing and storage capabilities (hereafter referred to as portable computers)
- Partners of the University who carry out work using University data
- those who access University systems from home or other remote locations using either privately owned, third-party-owned or University owned equipment; and,
- Staff who are responsible for systems that are accessed by users remotely.

Relevant requirements naturally extend to anyone else who is subjected to the Information Services Acceptable Use Policy who undertakes activities governed by this Policy.

It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, line managers are responsible for implementing this Policy within their respective departments and for overseeing compliance by staff under their direction or supervision. When collaborating with others outside our University, owners or stewards must ensure that collaborators are aware of and follow this policy.

Whilst it is recognised that compliance with all aspects of this policy cannot be 'policed', those

to whom it applies will be held to account for any aspect of non-compliance involving them that subsequently comes to light.

2. Data Storage

2.1. Requirement for Policy

In many cases the disclosure of University information would result in no impact, and the corruption or loss of University data will be little more than inconvenient or cause minor disruption.

However, some University information, such as personal data is sensitive and subjected to legislative control. The unauthorised disclosure, modification or loss of this type of information could result in damage to the reputation of the University or the prosecution of individuals for breach of the Data Protection Act 1998 or General Data Protection Regulations, May 2018, if it was found that the data had not been protected and managed in accordance with the requirements of The Act.

Likewise, some finance and research information may be sensitive. Certain research information may be the subject of a non-disclosure agreement imposed by the sponsor. If data of this nature was disclosed it could result in embarrassment to the University and the sponsor, potentially resulting in litigation and a loss of confidence which could adversely affect future research grants.

University information that is held or processed on systems outside of University premises is generally more exposed to being compromised, corrupted or lost than information that is held or processes on systems within University premises. This is down to various factors, such as:

- 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;
- physical security in the home may be lower than that of University premises, and some domestic properties may be more prone to burglary resulting in the theft of laptops and private computers;
- data can remain on mobile or remote systems after accessing University systems without some users being aware (i.e. cached web pages and e-mail attachments, data files 'synced' with cloud storage services such as OneDrive for Business);
- the University has no jurisdiction over privately owned equipment and when this has been used to access University information, data may be available to be viewed by unauthorised persons;
- the security of machines outside University 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;
- unserviceable privately-owned equipment containing University data is likely to be repaired through commercial arrangements where data may be viewed by repair staff during that process.

2.2. Affiliated Supporting Policies

This policy should be read in conjunction with the the:

- *Information Services Acceptable Use Policy* concerning activities which are and which are not permitted using University computer resources;

All users are required to familiarise themselves with the relevant aspects of the Acceptable Use Policy and are to comply with the specified requirements.

3. Data Storage, Backup and Retention

3.1. General principles of Data Storage

3.2. Office 365 and University File Storage

The University's Office 365 service can be used anywhere with an internet connection in a secure manner. The Office 365 OneDrive for Business service is the University's preferred repository for storing data and files.

User data stored in OneDrive for Business is held within the EU, and complies with Data Protection Law. Users can securely access this data remotely and view or edit it via online versions of desktop software such as Word or Excel and mobile apps.

External hard drives or USB sticks should not be used to access data or transport it. In exceptional circumstances access will be given to encrypted external storage via application to the IT Services Helpdesk.

As an alternative to OneDrive for Business, users may continue to store files in their University-Provided 'My Documents' folder or shared departmental drives such as the U: or Z: drive.

3.3. Backup

All users are personally responsible for ensuring that all University data they process (whether on University-owned or privately-owned devices) is regularly and frequently backed up. One way to ensure this to save all files to University managed storage systems such as OneDrive for Business accessed via the University's Office 365 Portal, their University-provided 'My Documents' folder, shared departmental drives such as the U: or Z: drive. Data stored in these locations will be regularly backed up by IT Services.

Removable media such as external hard drives or USB memory sticks should never be used to back up University data.

Backup arrangements should ensure that critical data is backed up daily, and that less critical data is backed up to the extent that loss of original source would be nothing more than a minor inconvenience.

The backups must be kept securely and remotely from the computer being backed up and without contravening Data Protection legislation.

People responsible for data backup and restoration should be suitably trained and supported as well as having the time to ensure this Policy is followed.

Any backup and restore scheme must be fully and securely documented.

The backup system must be tested and proven to work.

3.4. Data Archiving and Retention

Where data is archived for long-term retention, arrangements need to be made to ensure it remains accessible using either future technologies and software or that the systems and software on which it resided and operated are also preserved in an operational state.

When data no longer becomes needed or regulatory requirements mean that it has to be

disposed, this should be done in a timely and secure fashion.

4. Mobile and Remote Working Practices

4.1. Remote Access Service

The University's Remote Access Service is compatible with Microsoft and Macintosh systems. It can be used wherever Internet connectivity is available.

Alternatively, anyone who simply needs to access their email is permitted to use the University's Microsoft Office 365 service, which is independent of the Remote Access Service but which incorporates the same security functionality.

The Remote Access Service is able to access the same resources that users access from their University desktop/laptop whilst on campus. The connection provided is secure, with data traffic encrypted, and the data is saved in the respective user's 'My Documents' or departmental shared drive instead of on the local hard drive of the machine being used for the access. As the connection between the remote computers and the University server is secure (https), no data is cached on the remote computers.

This prevents potentially sensitive University data from being accessed by unauthorised persons should a computer be sold on, stolen, or taken to a third party for repair, or as a result of non- University employees being permitted to use the computer in question. Under no circumstances are these controls to be circumvented by transferring data via removable media, sending it as an email attachment or by any other means.

It is the responsibility of those leading project teams or research groups that are working on sensitive data, or under non-disclosure agreement, to ensure that appropriate controls are in place to protect that data. Where such work is being undertaken and mobile or remote access to respective data or systems is required, the IT Services Helpdesk is to be contacted so that advice can be given for an appropriate method of securely accessing such data.

4.2. Encryption of University owned portable computers

All university owned portable computers will have encryption enabled on the local storage of such devices. This will help prevent any data leakage as a result of loss or theft of a device.

4.3. The Creation and Storage of University Data on Privately-owned Computers

Privately-owned computers can be used to create or process personal or sensitive data, but only via University authorised means. These are currently OneDrive for Business (authenticated by University login credentials) and Remote Access.

The OneDrive for Business client must not be used on privately owed-computers to synchronise University data with that computer as this will leave copies of this data on such machines.

Privately owed-computers being used to create or access University data should have up to date anti-virus software and the operating systems should be fully updated with the latest security patches

4.4. Data Protection Implications - Remote Working Overseas

The Data Protection Act 1998 generally prohibits the international transfer of personal data (i.e. any data from which a living individual can be identified) into any country outside the

European Economic Area (EEA), unless that country is designated as being 'adequate'. At present, no country outside the EEA member states has been classed as adequate. (Annex A refers).

However, in certain circumstances, with specific controls in place, it is still possible for remote workers to process personal data whilst working overseas.

Any remote worker wishing to process personal data outside the EEA, without using the University's Remote & Mobile Access Service, must contact the IT Services Helpdesk to establish the feasibility of doing so and to determine the specific conditions that will be applicable to them should this be feasible.

4.5. Mobile Workers' Responsibilities

Users are responsible for the safekeeping and protection of University-owned portable computers that have been issued or loaned to them.

Users in possession of University-owned portable computers are responsible for preventing unauthorised persons from using them and they must not loan them to others without prior authorisation.

Users of privately-owned computers that are or have been used to create, process, store or access University data are responsible for ensuring that non-members of the University do not gain access to that data when using their computers.

4.6. Duty of Care

Reasonable care and due diligence must be taken to prevent or reduce the possibility of loss or theft of University-owned portable computers.

Mobile workers are to take heed of the environment in which they are working and apply appropriate common-sense measures to protect University-owned portable computers and University data on both University-owned and privately-owned devices.

Losses of, or damage to, University-owned portable computers may be investigated. Where negligence on behalf of the custodian has resulted in the loss or damage action may be taken in accordance with University procedures.

Whilst there are many situations in which mobile workers will find themselves operating, there are four main categories to consider:

- working within the University's premises;
- working outside the University's premises;
- working in transit;
- transporting portable computers.

Control requirements associated with each of these are outlined below:

Working within University Premises

University-owned portable computers are not be left unattended on the University's premises unless they are in a locked room or cupboard, with access restricted to local staff, or secured by an appropriate security device.

Working outside University Premises

When working outside The University's premises, mobile workers are to be extra vigilant and

apply appropriate precautions to protect portable computers in their care.

Working in Transit

Extra care must be taken when working in transit to prevent the disclosure or compromise of University information. Any unauthorised disclosure of personal information due to negligence on a user's part could make that user liable to prosecution under the Data Protection Act 1998 (or other legislation). This includes any case where details, which are governed by The Act, become public knowledge due to the theft of portable computers where it can be shown that the custodian was negligent in applying security controls. Sensitive University information must also be safeguarded against being viewed by unauthorised persons. Confidential data on University owned portable computers must not be accessed or processed in public places where it could be overlooked by anyone who is not authorised to view it.

Transporting Portable Computers

Constant vigilance must be applied to reduce the possibility of loss or theft of University-owned portable computers, or the disclosure of University information on either University-owned or privately-owned equipment, whilst in transit. If University-owned portable computers, or privately- owned equipment that contains University data, have to be left in vehicles, they are to be placed in the boot or out of sight and the vehicle locked.

4.7. Network Connectivity

Only University-owned and managed portable computers can be connected to the University Network. These are properly secured, patched and have other adequate security controls including anti-virus software.

Users of privately owned portable computers who wish to connect their devices to the University network are only able to do so wirelessly via Eduroam wireless network.

4.8. Security of Privately Owned Computers and the Protection of Data

Users, who access University information using privately-owned computer equipment, whether portable or static, are responsible for the security of them. In order to protect University information, such machines are to be protected by a firewall, operate anti-virus software (where necessary), and be kept up to date with security patches. Annex B gives guidance on the security of privately owned computers.

4.9. Incident Reporting

The loss of any University-owned portable information asset must be immediately reported to the respective line manager, and the IT Services Helpdesk.

In cases of both loss and theft of University-owned portable computers, an evaluation of the sensitivity or criticality value of the lost information may be carried to assess potential damage to the University's reputation and determine any counter-compromise actions.

5. Annexes

5.1. Annex A – Data Protection Act 1998 – International Transfer of Personal Data

The 8th Principle of the Data Protection Act 1998 does not impose any restriction on the transfer of personal data to EEA countries. At the time of publication these are:

Austria	Belgium	Bulgaria	Cyprus	Czech Republic	Denmark
Estonia	Finland	France	Germany	Greece	Hungry
Iceland	Ireland	Italy	Latvia	Liechtenstein	Lithuania
Luxembourg	Malta	Netherlands	Norway	Poland	Portugal
Slovakia	Slovenia	Spain	Sweden		

The following countries outside the EEA with their own data protection laws have been designated as 'adequate' by the European Commission:

Argentina	Canada	Guernsey	Isle of Man	Switzerland

United States of America (Safe Harbor list companies only).

For the latest up-to-date list of countries considered to be adequate, please see the European Commission's data protection website at
http://www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

5.2. Annex B – Security of Privately Owned Computers (including phones, tablets and any device capable of connecting to University IT services)

The use of privately-owned computers for University work imposes security responsibilities on the users.

Although many of the risks to University information or network resources are no different to those encountered by University-owned equipment, it is unlikely that the same processes and software are in place to protect privately-owned equipment. It is therefore important that steps are taken to protect privately-owned computers by:

- Maintaining up-to-date anti-virus software;
- Installing critical security patches for your device as soon as they become available;
- enabling a personal 'firewall' to protect your device from being hacked, especially if you have a broadband connection: and,
- deleting data which has been cached by your device
- Enabling disk based encryption where possible
- Phones and tablets should have a key code lock enabled

Anti-Virus Software

The important point to remember is that whatever anti-virus package you use it MUST be kept up-to-date if it is to remain effective. New viruses are appearing all the time and most vendors of anti-virus software release several updates to their software each week. Anti- virus software which is out-of-date is worthless.

Fortunately, you do not have to remember to update the software yourself as all these packages can be configured to periodically check for updates and download and install them without requiring that you do anything. It is recommended that you configure your anti-virus software to check for updates at least every day as it is not unknown for more than one update to be released within a single day.

Automatic Updates

New security vulnerabilities are being discovered in Windows software all the time and when they are Microsoft release updates in the form of critical patches.

Fortunately, you don't have to download these patches and manually install them yourself. Windows incorporates a built-in feature called Automatic Updates.

When this is enabled your PC will periodically check with Microsoft's servers to see if there are any new critical patches available. If there are it will download and install them for you. The extent to which you are aware that this is happening is configurable by you. For information on how to enable the automatic update feature select **Help and Support** from the **Start** menu. Then search the Windows help system for 'Keeping Windows up-to-date automatically'. This will take you to step-by-step instructions on how to enable this feature.

The latest full versions of operating systems are more secure than their predecessors, so we recommend that you use the latest version of your computers operating system where possible.

For example, Windows 10 is more secure than Windows 7 or Windows 8.1.

Internet Connection Firewall.

Home PCs with network connections are deliberately targeted by people who wish to misuse them. Historically, home computers have lacked the network protection and automatic updating systems that are found on enterprise systems. One way of enhancing the protection of home computers is to utilise an Internet connection firewall.

A firewall is a piece of software or hardware, or a combination of both which runs on your PC and constantly listens for attempts by people on the network to make possibly illicit connections to your it. If you haven't explicitly authorised this activity it will block such attempts. It's particularly important if you have a broadband connection to the Internet that you operate a firewall.

Without a firewall and anti-virus software that checks for Trojans it will be easier for people to install software on your PC which will then give them remote control of it. Once they have control of your PC they potentially have access to the University's information assets.

Windows has an in-built personal firewall which works fine, although more effective products can be bought. For information on how to enable the Windows Firewall select **Help and Support** from the **Start** menu. Then search the Windows help system for 'Firewall'. This will take you to step-by-step instructions on how to enable this feature.

Internet Cache

As an employee, you have an obligation to safeguard the security and confidentiality of the University's sensitive information assets. Many people are unaware that when they view documents through the web, or as an email attachment, a copy of that document will be written to the hard disk of the PC being used, and they don't have to explicitly save documents to the hard disk in order for copies to start accumulating there. Note, when using the University's Remote Desktop Service data is not cached.

When a PC has been used to access non-secure web sites it will have cached information stored on the local hard disk unless measures have been taken to remove this first. This may be available to others should it be taken to be repaired, or subsequently disposed of.

When you view a non-secure web page, your web browser, e.g. Internet Explorer or Chrome, always writes a copy of that page to an area known as a cache. The next time you view it the browser can then read it from the cache rather than going back to the original website. This speeds up web surfing but in it also means that the information has been copied from its domain on to the PC's hard disk.

Likewise if you view a word document or an Excel spreadsheet from a web page or one that has been sent to you as an email attachment, your PC will keep a copy locally even though you may never have been asked to save it.

You should configure your internet browser to delete the contents of your Temporary Internet Files folder each time you exit from the browser.

You are also encouraged to check your computer for spyware etc. periodically, by using proprietary software.