File Handling Guidelines

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	06/07/2017
V 0.2	Andrew Clarke	General updates following PWG comments Also, addition of FigShare and extended matrix.	17/07/2017
V 1.0	Andrew Clarke	CISA Board amendments (ref CISA-1112.1) – file ownership	04/09/2017
V 1.1	Andrew Clarke	OneDrive for Business added	06/08/2019
V 1.1	Andrew Clarke	Annual Review	01/08/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 04 Sep 2017
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 04 Sep 2017
Distribution:	ALL

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

The purpose of this Advisory is to outline the acceptable ways of handling information assets and file storage at Brunel University London. These rules are in place to protect the employee and Brunel University London. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, and legal issues.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber & Information Security Manager	Is responsible for maintaining the Advisory and to ensure that the Advisory continues best practice and ensuring compliance with legislative and regulatory requirements.
All Users	It is the responsibility of all users of the Brunel University London's I.S. services to read and understand this Advisory. This Advisory may be updated from time to time, in order to comply with legal and Advisory requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.1.3 Acceptable use of assets

1.4 Scope

This Advisory applies to employees, contractors, consultants, temporaries, and other workers at Brunel University London along with Students.
This Advisory applies to the use of all Brunel University London electronically stored information. It also extends to information held on behalf of third parties and partners.
This Advisory also applies when using your own device to store, access or process information on Brunel University London Information Systems.
This Advisory applies at all times when using Brunel University London information Systems and not just during your normal working hours.

All employees, contractors, consultants, temporary, other workers and students at Brunel University London and its subsidiaries are responsible for exercising good

judgment regarding appropriate use of information in accordance with Brunel University London policies and standards, and local laws and regulation.

2.0 File Handling

Staff and students at Brunel University London have access to highly-resilient safe and secure file storage. All users have personal storage space - your home drive (H: drive) and your OneDrive for Business in the cloud.

Staff also have access to shared storage space e.g. G: drive and J drive - the shared areas are normally used for team/departmental files.

Network folders such as H:, J: and G: drives can be accessed when off-campus (e.g. at home, abroad) by connecting to the University network through the Virtual Private Network (VPN), AnyConnect VPN.

AnyConnect VPN does not work on campus and is not required in halls of residence.

<Access using AnyConnect VPN>

You should save your BUL files to your H: drive, the OneDrive for Business repository or a shared area e.g. G: drive or J: drive.

You should not save files on your Windows desktop, the C: or D: drive as these are not backed up - and the files may be vulnerable to damage or loss from fire, theft, hardware faults or operator error.

If you do save files to the Windows desktop, C: or D: drive, a personal device or removable storage device, ***it is your responsibility*** to ensure that you have secure copies of any important files you choose to store there.

My Documents

Traditionally, My Documents are located on the physical and local disk drive on the desktop or laptop client device along with the windows Operating System.
Although extremely convenient for storage, access speed and accessibility wherever you are, there are inherent issues with local storage, such as data loss owing to hardware failure and backups, both of these issues are compounded by malware and ransomware.

The University has re-directed My Documents to the network H drive where you where you can save your own work. This is known as your file-store and it is located on the H:\ drive (Home).
Always save your work to the H:\ drive, as this is backed up and can be recovered if necessary in the event of ransomware.
All data stored in this area must adhere to the Brunel Acceptable Computer Use Policy (BACUP) and all legal requirements.
Do not save to the C:\ drive or the D:\ drive, as you could lose your work.

1) **University Personal File Storage:**

- H: drive

All staff and students have a personal storage area on secure university servers – your H: drive. The standard H: drive quota for staff is 3GB and students 500MB- additional storage is available on request. A warning will be given when usage meets or exceeds 95%.

To optimise use of your quota, you can compress (zip) rarely used files using 7-Zip.

Off-campus access to your H: drive is via the Virtual Private Network (VPN)

Features:
- Personal;
- Secure;
- Not shared;
- Backup;
- Access off-campus;

2) **University Shared File Storage:**

- G:, J: Drives
- Unix personal drive, mainly used for Webhome (if someone wants to create a public webpage) but also some Admin applications for transferring data;

Features:
All staff have access to their Department or service shared drives e.g. G: J: etc.
Off-campus access to your shared drives is via the Virtual Private Network (VPN).
- Departmental/University;
- Secure;
- Shared;
- Backup;
- Access off-campus;

There are particular risks with using the network file shares, which include:
- Ransomware attacks will likely cover the entire share;
- We have some very large shares (e.g. Admin file store for all professional services directorates);
- Permissions management is complex and inherits legacy permissions that may have expired;
- Folders named by individuals' names, many of whom have since left the university but the content remains;

SharePoint remains the recommended solution for University storage.

3) **BUL OneDrive for Business:**

All BUL staff with an email account have access to their own BUL OneDrive for Business[1]. Your OneDrive gives you 1 TB of storage space in the cloud.

[1] OneDrive for Business is a cloud storage tool that allows you to store and protect your files, share them with others, and get to them from anywhere on all your devices.

Never share or store University Confidential/business critical BUL information on private third party cloud services like Dropbox, YouSendit, personal (i.e. not University) OneDrive, ICloud, Google Drive.

Confidential/business critical data should be stored on secure University systems. Data stored on your BUL OneDrive is held in Europe to comply with UK privacy laws. Data stored in private cloud accounts may be held anywhere in the world - with no accountability if the company loses your data.

You can access OneDrive from the Office 365 Web App – click the app launcher in the top left of the Office 365 window and you will see it displayed in the apps pane.

OneDrive is useful for current pieces of work – particularly files where you are collaborating with individuals or groups both within and out with the University.

You can access your OneDrive from anywhere via the internet (go to Office 365).

Features:

- Personal;
- Secure;
- Shared;
- Version Control;
- Support a large variety of files;
- Edit documents without downloading them to your computer;
- Share through the Web app;
- Access off-campus;

4) BUL Dropoff:

The Dropoff service provided by the University's Information Services is an extremely secure method of information collaboration and is ideal for those people who wish to transfer large files to other people or groups and is accessible for anyone with a valid email address. The service works for people inside and outside the Brunel domain and has a maximum upload limit of 2GB.
Files placed in the Dropoff are only there for a limited amount of time and should not be used to permanently store files so data will need to be transferred to an alternative storage location of the information is required for a longer period of time.
Once the file has been uploaded the recipient will be sent an email with the details of the drop-off and a unique 16 character passcode that must be entered to claim the download.
After fourteen days the drop-off will expire and each night be purged from the Dropoff.

If you need to share files that are either larger than 2GB, or perhaps need to be streamed (such as podcasts or videos) Information Services can help you. Please get in touch with Information Services with your requirements.

Features:

- Personal;
- Secured;
- Shared;
- Support a large variety of files;
- Files must be downloaded to the computer, so nothing is opened while online;
- Access off-campus;
- 14 day file expiration;

5) SharePoint:

Authorised staff can store information on the university intranet site - SharePoint. SharePoint pages can be viewed by all BUL staff. Non-BUL users can be given access to SharePoint on request i.e. for project work with and on-behalf of the university.

Information that you want to make available to all staff in the university can be added to SharePoint e.g. policies, staff forms e.g. expenses claims, and system information and help

Each College and service has a SharePoint site. You can access SharePoint off-site without using the VPN.

Features:

- Personal;
- Secured;
- Shared;
- Version Control;
- Support a large variety of files;
- Edit documents without downloading them to your computer;
- Share through the Web app;
- Access off-campus;

6) BUL MySite:

MySites are a version of OneDrive that are hosted on BUL infrastructure and are not cloud-based. If you need to send files to someone with a Brunel network account, this is best achieved using MySites.

MySite provides staff with a secure online area to store and share documents, manage tasks and use IntraBrunel's social features to keep track of activities on other IntraBrunel sites or documents.

All files stored in your MySite are private by default, except for files placed in the special 'Shared with Everyone' folder. You can share files and collaborate on documents with colleagues by amending the privacy settings of individual files.

The default quota size for a MySite is 250MB with a single file size limit of 100MB, this is set deliberately small to encourage the majority of collaborative work to be conducted within the provided IntraBrunel Team and other Collaboration sites.

Using your MySite also removes the need for you to email files to your personal email addresses (both University and internet email accounts such as Hotmail and Gmail) if you want to work on them on your home computer, as files can be accessed from any computer or tablet device via a web browser.

It is expected that people will use their MySites alongside a Dropoff (or Microsoft BUL OneDrive) Office365 account instead of replacing it. Both allow you to store and access files from any computer via a web browser.

However, because your MySite keeps documents on Brunel premises and always under Brunel's control then you do not risk violating any data protection laws which may apply

to some of your documents, as long as you don't share sensitive documents with the wrong users.

The big difference with Dropoff is that currently you can only share files stored on your MySite with other Brunel staff, meaning they will need a Brunel network account to be able to access the files you want to share.
The intention would be to migrate MySites to OneDrive for Business once the OneDrive service becomes operational.

7) **Brunel Figshare**

Brunel.figshare.com is the University's web based research data repository (RDM) and data registry, based on the figshare for institutions platform. It has been created to help Brunel researchers comply with research data policies which require the data underpinning publications and data of long term value to be made openly accessible. Figshare offers 'Projects' spaces to facilitate collaborative working and data sharing between research group and consortium members across different institutions.
It is essential that a check is made regarding data sharing requirements of your funder and/or your publisher before using Figshare. Further information on funder requirements can be found on the Research Data Management webpages.

Where data can be shared figshare allows you to upload data and either make it public, or keep it under embargo until a specified date, when it can be released.

Where data cannot be shared (e.g. personal data, non-digital data, embargoed or confidential data), or datasets are too large to be held online or the data is already stored elsewhere, you must create a Metadata record describing the data and terms of access

Every dataset must have a corresponding published Metadata record, unless contractual restrictions apply, and a Digital Object Identifier (DOI) must be obtained and included in the data access statement on associated publications.

It will not normally be necessary to upload complete raw datasets – data which has been distilled for publication is acceptable.

Collaborate and share data on 'Projects' workspace

8) **Cloud File Storage:** (not recommended, University Confidential information must not be stored on these repositories)

- Personal Microsoft OneDrive
- Google Drive
- SugarSync
- Ubuntu (linux as well as Windows)
- SkyDrive
- Mozy
- Amazon Cloud Drive
- SpiderOak
- Wuala
- Minus
- iCloud
- Syncplicity
- LiveDrive

Features:

- Personal;
- UnSecured;
- Shared;
- Version Control;
- Support a large variety of files;
- Edit documents without downloading them to your computer;
- Share through the Web app;
- Access off-campus;

9) Cloud Collaboration Storage: (not recommended, University Confidential information must not be stored on these repositories)

- Dropbox
- Box
- MEGA
- pCloud
- MediaFire

Features:

- Files must be downloaded to the computer, so nothing is opened while online;
- Shares from desktop app;
- Unsecured
- Personal;
- Shared;
- Version Control (30 days);
- Support a large variety of files;
- Share through the Web app;
- Access off-campus;

Cloud collaboration storage should only be used as a last resort for collaboration owing to the fragmented nature of individuals each seeking their own solution. This is a disproportion costs to the University and is completely unmanaged and unverifiable.

10) Removable Media (USB devices) Pen Drives, External Hard Drives etc.:

Staff should not store University Confidential or protect work files on personal devices and drives unless encrypted .The physical nature of removable media such as USB keys and portable hard drives, means that these can easily be misplaced or stolen, leading to a loss of availability or confidentiality of the stored files. Recommended alternatives include

- SharePoint
- Secure shared areas (via VPN for off campus)
- Microsoft OneDrive for Business

These options ensure that your files are kept safe as well as significantly reducing the risk of loss or theft.

If you do use removable media: -

- Never save the master copy of your files on the device
- If storing personal or confidential information, the USB key or hard drive should always be encrypted (see below)

11) SFTP (SSH File Transfer Protocol):

The SFTP allows for a range of operations on remote files which make it more like a remote file system protocol. A SFTP client's extra capabilities include resuming interrupted transfers, directory listings, and remote file removal.
SFTP provides secure transmission that protects the username and password, and encrypts the file content but when sending files to other SFTP servers, care should be taken as any third party account with access to the file repository will have access to the contents of the files deposited.

SFTP is a secure method of information exchange and is appropriate for those people who wish to transfer large files to other people or groups and is accessible for anyone with a SFTP Server access. The service works for people inside and outside the Brunel domain.

FTP is an unsecure method of file transfer and should not be used as users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

2.1 Preferred File Handling Matrix

Internal - Personal	**Internal – Collaboration (Shared)**	**External (Cloud) – Personal Storage**	**External (Cloud) – Collaboration (Shared)**	
H: - MyDocuments	**SharePoint**	**BUL Microsoft OneDrive**	**BUL Dropoff**	BUL Preferred solutions
MySite	**Network – G: drive**		**FigShare**	
USB Pen Drive	MySite	SkyDrive	Dropbox	
	USB Pen Drive	iCloud (Apple)	BUL Microsoft OneDrive	
		Google Drive	iCloud (Apple)	
		Mozy	Google Drive	
		LiveDrive	MediaFire	
		Amazon Cloud Drive	pCloud	
		SugarSync	Ubuntu (Linux)	
		Ubuntu (Linux)	MEGA	
			Box	

2.2 File Storage Handling Features Matrix

Preferred University Solutions Matrix	**Storage limit / file size**	Shared – BUL (@brunel.ac.uk)	Shared - External	Backup	Secure	Access permitted off-campus (VPN)	ACL - Access Control	Editing off-line	Windows, Apple + Linux access	File System / Structure	Document Mngmnt / Document Auditing	MS Office integration	Syncing	Cost	File Version Control
My Documents (H:)	**3GB (500MB students)**	✗	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗
SharePoint	**Limited**	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
Network Drives (G:)	**Limited for academics**	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗
MySite	**250MB / 100MB**	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
BUL Dropoff – ***temporary 14 days***	**2GB**	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
BUL Microsoft OneDrive for Business	**5TB**	✓	✓	✓ **(30 days)**	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓
Personal Solution															
Dropbox	**2GB (paid Dropbox+ - 1TB)**	✗	✓	✗	✗	✓	✓	✓	✓	✓	✗	✗ **(paid Dropbox+)**	✓	✓	✓ **(30 day)**

3.0 File Ownership

What are the responsibilities of the data owner?

The file owner is responsible for setting up policies to allow specific individuals to see and update the file. Usually, a person's role determines access. For example, anyone in the accounting department can view the accounting file, but only lead accounting analysts can add new accounts.

The file owner is also responsible for determining who has access to the file, how the file should be secured, how long the file should be retained, what the appropriate disposal methods are, and whether the file should be encrypted.

The file owner may appoint an administrator to do the daily tasks associated with these responsibilities. For example, the file owner may appoint someone to approve daily requests to access the file. The appointed person will act under the direct instructions of the file owner.

Unfortunately, IS often ends up being the de facto owner of the file. Although the IS department can be the custodian of the file, it should not be the owner. Employees in IS generally do not know how important the file is to the University, how the file is to be used, and which people (or roles) should access the file.

Another reason IS should not be the owner as well as custodian of the file is separation of duties. If IS decides who has access to the file and then administers that access, there are no checks and balances to ensure that access control policies are being followed or that inappropriate access is not being assigned.

IS's role is usually that of file custodian. The custodian is responsible for implementing the policies set by the file owner. For example, IS is usually responsible for ensuring that the files access controls (such as *PUBLIC authority) are set per the file owner's requirements. IS is also responsible for backing up the file as well as properly disposing of any electronic copies of the file in the department's possession.

Appendix A – Brunel University Data Backup Policy

- Information Services Backup Policy for Windows Data
  Information Services backup user data overnight and at weekends, this time is the backup window. The backups are kept for a maximum of six months, this is the backup cycle: for G: and H: Drives
  - ✓ FULL backups pick up all closed saved files on the server;
  - ✓ INCREMENTALS pick up all newly created or modified saved and closed files created since the last backup;

- Network drive (H: - My Documents) and department drives (G:) backups
  Backups on these servers run each night:
  - ✓ FULL backups at the weekend;
  - ✓ INCREMENTALS each night, these backups are kept on-site for 35 days;
  - ✓ An additional FULL backup is run every 4 weeks and kept off-site for 175 days;

Appendix B – Personal Backups

Computers are easily replaceable, but data loss can be irreversible, particularly with Ransomware.
Here are some advisories to help you ensure that your data isn't lost if your data is lost.

- **Backup set A, Backup set B**
  Make two backups, not just one. If you have problems while overwriting a previous backup, this will ensure you still have one backup copy available, as well as the original data. Three copies of the data (the original and backup sets A and B) are much safer than just two.

- **Optical Media**
  CDs or DVDs are not recommended for backing up irreplaceable data. Unless the blank optical disk is of high quality, and is handled and stored with great care, data written to it may be lost or the optical disk may become unreadable.

- **USB flash Drives**
  USB flash Drives are suitable for backing up smaller amounts of data. They are reasonably robust, but can only sustain a limited number of write cycles. This limit may be about 1,000,000 writes, but note that may not mean to each memory cell, so a common USB flash drive life may be shorter, perhaps as low as 50,000 writes. Despite this limit USB flash drives may be relied upon for a few years, depending on the cycle of use.
  Do consider that, owing to their size, these are easily misplaced or lost and unless encrypted, are easily stolen resulting in potential data breach.

- **USB external hard drives**
  USB external hard drives are suitable for backing up many gigabytes or terabytes of data. They are fast and reasonably robust. If they are handled correctly, USB external hard drives can be relied upon for a few years, depending on the drive specifications and the level of use.
  External Hard Drives should not be left connected to a client device but removed after backup as they have the potential to be attacked by malware (Ransomware) thus negating the very purpose of the backup.

- **Encrypt data with VeraCrypt**
  If your data is subject to the Data Protection Act, or otherwise sensitive or secret, it may be worth using VeraCrypt (downloaded from VeraCrypt). This application can be used to encrypt your data, or even the entire data drive. If you deal with data covered by the Data Protection Act, you should speak to the University's Information Access Officer to confirm you are handling the data properly.

- **Offsite Backup**
  One set of backups should be kept in a separate physical location from the computer that stores the original data. In this manner disasters such as fires, floods, etc. may destroy the computer with the original data, and Backup set A, but Backup set B is highly unlikely to also be affected. For this reason all backup data from the Brunel network is offsite.

- **Test Restore**
  It is important to regularly run a test restore from your backup, to prove the media is still valid. Eventually the backup media will reach the end of its useful life, at which point it must be replaced by a fresh data storage device.

- **Backup Software**

If you use a proprietary backup program, the licence must still be valid when you finally need to restore the data. If the backup software is discontinued, you may lose access to your data. It is safest to simply copy your data, to guarantee that you will not be denied access due to 'vendor lock-in.'

- **File Formats**
  You should consider carefully which file formats you choose to store, and ensure you will still be able to recover and read them in the future. If you have old documents saved using e.g. Wordperfect6.1 for DOS, you must be able to run that program to be certain that you can use that data after it's restored.

- **Data Loss**
  Data loss refers to the unexpected loss of data or information, this can occur for many reasons including hardware failure, software failure, or power failure. For this reason, Information Services strongly advises against the practice of saving data to the local drives of your PC. Users are encouraged to always save data to their network drive.

If you suffer from data loss on the local drives of your PC, Information Services may be able to advise on the best course of action but are currently unable to provide a data recovery service.

Appendix C – Information Classification

University information stored both physically and electronically, must be classified to identify what type of information is contained within the document.
The University classifies information into three levels (University Confidential, Protect and Unclassified):
Ref: Information Classification Procedure

CATEGORY	DESCRIPTION	Sample Documents/Records
UNCLASSIFIED	Information that may be broadly distributed without causing damage to the University, its employees and students. These documents may be disclosed or passed to persons outside the organisation.	Marketing materials authorised for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices
PROTECT	Information whose unauthorised disclosure, particularly outside the University, would be inappropriate and inconvenient.	Most University information falls into this category. Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorised release), transaction data, productivity reports, , contracts, Service Level Agreements, internal vacancy notices, intranet Web pages
UNIVERSITY CONFIDENTIAL	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organisation without the explicit permission of a senior manager.	Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal IDENTIFIABLE information (PII) - such as employee HR records, Social Security Numbers, SITS records, disciplinary reports, most accounting data, Exam papers (before use) other highly sensitive or valuable proprietary information

For research data comprising participate information or animal welfare/BIO data, the Research Ethics Code of Practice must be adhered to irrespective of whichever file storage solution is selected.

All Personal Identifiable Information (PII) data must be anonymised to the research level. For further advice, see Information Access Officer.

	UNCLASSIFIED	**PROTECT**	**UNIVERSITY CONFIDENTIAL**
University managed electronic storage (MySite, Dropoff, network)	Normal Do not leave unattended on screen - lock screen	University's network: restricted access by defined user/user groups to specific areas **Mobile working:** Minimum encryption protection on University owned mobile storage device, preferably access directly through remote network access (VPN) Do not leave unattended on screen - lock screen	University's network: restricted access by defined user/user groups to specific areas Mobile working: Minimum encryption protection on University owned mobile storage device, preferably access directly through remote network access (VPN). **Mobile devices** must have Full Disc Encryption (FDE) using complex password. Do not leave unattended on screen - lock screen
Office 365	Normal Do not leave unattended on screen - lock screen.	University authorised OneDrive for business; Office 365 Groups; SharePoint Online; Office Apps (Word, Excel, PowerPoint, OneNote) Skype for business, Yammer, Sway and Forms not permitted Do not leave unattended on screen - lock screen.	University authorised OneDrive for business; Office 365 Groups; SharePoint Online; Office Apps (Word, Excel, PowerPoint, OneNote) Skype for business, Yammer, Sway and Forms not permitted Do not leave unattended on screen - lock screen.
Electronic Cloud (Internet) Storage - excluding University Office365. (e.g. Dropbox, Google Drive, Copy, Box, Personal MS OneDrive, iCloud, Sync.com, E-Box, Tresorit, owncloud, Viivio)	Normal Do not leave unattended on screen - lock screen.	Not to be stored on Cloud Storage unless University authorised Office365.	Not to be stored on Cloud Storage unless University authorised Office365.

	UNCLASSIFIED	**PROTECT**	**UNIVERSITY CONFIDENTIAL**
Electronic backup	Backup stored in locked cabinet	Backup stored in locked cabinet	Backup stored in locked cabinet
Removable and storage media (CD-ROMS, USB storage)	Normal procedures	Not to be stored on personal removable and storage media, only those provided by the University – must be encrypted to at least 256-bit AES cipher encryption	Not to be stored on personal removable and storage media, only those provided by the University – must be encrypted to at least 256-bit AES cipher encryption and FIPS-140-2 level