Information classification and handling policy and guidelines

Lady Margaret Hall

CONTENTS

PURPOSE

Imagine waking up to discover that information that you process about people or for the College/University has fallen into the wrong hands. At this point several uncomfortable situations could start to unfold depending on the scenario. Either way, you are part of the situation and there could be varying degrees of effect on you, the people around you, the College/University and individuals who place trust on you.

We all need to treat Information Security with the importance it deserves and make use of the tools available to us in the correct way. The purpose of this document is to provide Members of [College] with both a policy and guidelines in the use of a variety of storage services and mediums, both within and outside the University.

WHAT INFORMATION ARE WE CONCERNED ABOUT? (CLASSIFICATION)

University data

- Data that has been provided by the University. The University may provide rules surrounding the use of data provided by them.

College data

- Data that has been provided to or sourced by the College, including data provided by the University or any outside source that is deemed confidential. This may include Highly Protected or Protected data as defined below.

  College data can be then split down into the following:

Highly Protected data

Teaching and research

- Sensitive Personal Data relating to students and participants
- Mass (>1000 records) Personal Data relating to students and participants
- Patient identifiable data
- Sensitive research data
- Intellectual Property
- Details of animal houses
- Examination papers (under preparation)

Development and Fundraising

- Sensitive Personal Data relating to alumni and donors
- Mass (>1000 records) Personal Data relating to alumni and donors

Operations (HR/Finance/IT/Estates)

- Unpublished financial accounts
- Payment card data
- Passwords
- Sensitive Personal Data relating to staff and visitors
- Mass (>1000 records) Personal Data relating to staff and visitors
- Details of hazardous and radiological materials

Admissions and Outreach

- Sensitive Personal Data relating to applicants or general public
- Mass (>1000 records) Personal Data relating to applicants or general public
- Any Personal Data relating to children

Protected data

Teaching and Research

- Personal Data relating to students other than basic student data (or >100 basic data records)
- Any Personal Data relating to participants
- Research contracts
- Marks, prizes, appeals and complaints
- Unpublished research papers
- Course and exam information
- Student discipline information

Development and Fundraising

- Any Personal data relating to alumni and donors
- Project research and analysis
- Gift administration

Operations (HR/Finance/IT/Estates)

- Personal Data relating to staff other than basic staff data (or >100 basic data records)
- Any Personal Data relating to visitors
- Staff performance and discipline information
- Financial records and transactions
- Information on Intranets, network shares or SharePoint
- Internal governance documents or reports
- Meeting agendas & minutes
- IT system and infrastructure information
- Usernames and IDs
- Supplier contracts

Admissions and Outreach

- Any Personal Data relating to applicants or general public
- Applications, aptitude tests, interview notes, outcomes
- Funding assessment information
- Information relating to commercial activities

If you are unsure about the definitions above, then please contact either the source of the information you are processing or the College Data Protection Officer (DPO). For the purposes of this document, personal data is assumed as being part of both College and University sourced or controlled data.

HOW SHOULD INFORMATION BE HANDLED?

Departments, more specifically process owners, are responsible for determining information handling rules. Guidelines per classification level are given below:

Store, Process, Share ...	Highly Protected	Protected	Public
Where	• College/University premises, ICT Infrastructure or approved third parties. • College issued/controlled devices only.	• College/University premises, ICT Infrastructure or approved third parties. • Can be transported in encrypted form with the Treasurer's permission. • Can be accessed on personal devices that satisfy College Information Security Policy requirements	• Anywhere.
How	• Approved methods only (see below). • High levels of physical security with monitored access. • 'Off-Site' usage must be explicitly authorised by the Treasurer. • Minimal number of copies permitted with full audit trail. • 2-factor authentication for remote access. • Explicitly approved third parties with appropriate contractual agreements and Third Party Security Assessment. • Strict policies and procedures for secure disposal/deletion. • All data sharing must be explicitly authorised and files encrypted using appropriate password protection before being sent. • Passwords for decrypting documents are sent via alternative means. • Physical copies kept in locked drawers, filing cabinets or equivalent. • Physical copies only sent via recorded delivery or courier. • In accordance with appropriate GDPR retention schedule.	• In accordance with baseline security standards. • Secured (e.g. in a locked cabinet) when out of the office. • Remote access permitted • Contractual agreements for third party access as per College's Supplier agreements. • In accordance with appropriate retention schedule.	• Any method. • In accordance with appropriate retention schedule.
Who	• Tightly restricted groups of authorised persons only. • Approved and assured third parties only.	• Authorised personnel (including third parties) only.	• Anyone.

Information classification and handling policy and guidelines

To comply with the Information Handling Rules users must adhere to the following practices:

	Highly Protected	Protected	Public
Using email	• Double-check recipient address. • Use blind copy (bcc) when mailing large numbers of recipients. • Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.	• Double-check recipient address. • Use blind copy (bcc) when mailing large numbers of recipients. • Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.	• Double-check recipient address.
File transfer	• Internal College or University tools permitted (e.g. SharePoint or OxFile). • Encrypt files (e.g. Microsoft Encrypt with Password or 7-zip) and share passwords separately via trusted means	• Internal College or University tools permitted (e.g. SharePoint or OxFile).	• Any tool permitted.
Post	• Permission from Treasurer required. • Sealed envelope with sender details. • Sent by recorded delivery or courier. • University Mail Service not	• Sealed envelope with sender details. • Normal external mail and University Mail service permitted.	• Any method permitted.
Cloud Storage	• Follow the advice in the next section of this document.	• Follow the advice in the next section of this document.	• Any tool permitted.
Paper Storage	• Locked drawers, filing cabinets or equivalent in restricted-access College premises.	• Desks and offices in restricted-access College premises • Locked draws, filing cabinets or equivalent in unrestricted-access College premises or off site.	• Anywhere.
College provided network file stores/drives	• Within restricted-access drives/folders. • Encrypt files with Passwords. • Share passwords separately via trusted means.	• Within restricted-access drives/folders.	• No restrictions.
Portable storage	• Permission from Treasurer required. • Encrypt either specific files or the whole device. • Share passwords separately via trusted means. • Kept in locked drawers, filing cabinets or equivalent when not in	• Permission from Treasurer required • Encrypt either specific files or the whole device.	• No restrictions.
College Managed Devices	• Permitted.	• Permitted.	• Permitted.
Personally Managed Devices	• Only via Remote Access.	• Only via Remote Access.	• Permitted.

CLOUD STORAGE

WHAT IS IT?

The phrase "cloud storage" refers to third party online storage services such as **Google Drive, Dropbox, iCloud and OneDrive**. Files processed on these services can usually be accessed via any web browser and often have the capability to be "synchronised" to multiple computers and mobile devices such as mobile phone and tablets. They may also have facilities for sharing files with other people. This makes cloud storage a very useful way of accessing, working with and sharing information. The intention here is not to tell you that you cannot use such services, rather that you should consider how they are used when processing University, College and personal information.

WHAT ARE THE RISKS OF USING CLOUD STORAGE?

Cloud storage introduces several risks to the security, privacy, copyright and retention of University and College data.

Before using cloud storage for work, users must consider if the usage is appropriate.

The main risks when files are stored in public cloud storage are that:

- The University can no longer guarantee the quality of access controls protecting the data.
- The location where the data is stored may not be guaranteed as remaining in the European Economic Area (EEA) and so may not meet Data Protection Act and GDPR requirements for personal data.
- Using cloud storage to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment.

CONSIDERATIONS BEFORE USING CLOUD STORAGE

When considering whether or not to use cloud storage several questions need to be asked:

- Is any of the data you intend to process within the categories above?
- If you are sharing data, who are you granting access to?
  (are they members of the University or external)
- Are you using it to synchronise files between both work and personal devices?
  (is each device secure/encrypted)
- Is there a University or College alternative available?
  (not Dropbox, Google drive, iCloud etc)

WHERE CAN I PROCESS AND /OR STORE DATA (UNIVERSITY-LINKED CLOUD STORAGE SERVICES)?

	Nexus365	Nexus	OneDrive	OnTheHub by Kivuto
Service name and description	Nexus365 OneDrive for Business	SharePoint OneDrive (on Premise) mysite.nexus.ox.ac.uk	OneDrive Personal	OneDrive for Business Through Kivuto
Process University data?	Can be used for **temporarily processing** University data, except where prohibited by the Data Controller[1].	Can be used for **temporarily processing** University data, except where prohibited by the Data Controller.	No	No
Process College data?	Can be used for **temporarily processing** College Protected data[1], except where prohibited by the Data Controller. College Highly Protected data must be encrypted with Passwords. Share passwords separately via trusted means.	Can be used for **temporarily processing** any College Protected data[1], except where prohibited by the Data Controller**Error! Bookmark not defined.**. Must not process College Highly Protected data must be encrypted with Passwords. Share passwords separately via trusted means.	No	No
Storage available	5TB	2GB (can be extended)	5GB	1TB (can be extended to 5TB)
Data location	UK Datacentre(s)	On University Premises	Worldwide	EU Datacentre(s)
Backup	Deleted items will stay in the recycle bin for 90 days unless emptied. The second-stage recycle bins keeps items for a further 30 days. Overwritten documents may be	Deleted items are held in the recycle bin for 30 days. A chargeable service can be used to restore some older items. This is not guaranteed. Unless specifically setup, versioning is not	Deleted items are held in the recycle bin for 30 days. The second-stage recycle bins keeps items for a further 30 days. If the recycle bin is full, the oldest items will be automatically deleted after three	Deleted items are held in the recycle bin for 30 days. The second-stage recycle bins keeps items for a further 30 days. If the recycle bin is full, the oldest items will be automatically deleted after three days. Overwritten

[1] For support staff, please check with the policy owner or the DPO if you are unsure if processing information is not allowed. For academic staff, check with the data owner for the data you are processing; this might be at College, your department or research/funding body.

	recoverable through restoring a previous version.	setup by default. Overwritten documents are not recoverable.	days. Overwritten documents may be recoverable through restoring a previous version.	documents may be recoverable through restoring a previous version.
Authentication (how to log in)	University Single Sign-On (SSO)	University Single Sign-On (SSO)	Personal Microsoft Account	University Single Sign-On (SSO) to signup. New credentials provided and held in Azure AD (@oxforduni.on.microsoft.com)
File sharing possibilities (not an indication of whether or not to be used)	Anyone (internal or external to the University)	Internal University card holders only	Anyone	Anyone
Support	IT Services /College ICT	IT Services /College ICT	Microsoft	Kivuto/ Microsoft
Data access/ Account expiry	Account expires as soon as you leave the University. Anyone who has been given shared access to files will be able to for further 2 months.	Account expires as soon as you leave the University. IT back up access for further 60 days.	Perpetual unless account removed by owner.	Annual subscription, requires annual renewal. When you leave the University the account expires when next due for renewal.
Key Advantages	Integrated part of University Office365.	On-premise. Allows you to use SharePoint libraries and lists within your OneDrive space (such as shared calendars, custom lists etc).	As this is tied to your personal account, the space stays with you as long as your account stays active.	
Disadvantages	Not suitable for data that is required to be stored or processed on premise. Individuals are responsible for moving their data they want to keep out before they leave.	No file sharing with external users. Individuals are responsible for moving their data they want to keep out before they leave.	Can share content anonymously but not necessarily securely.	Has no associated email address.

USE OF NEXUS 365 ONEDRIVE AND NEXUS SHAREPOINT

MORE ABOUT USAGE

OneDrive for Business is certified against the internationally recognised ISO/IEC 27001:2013 standard for managing information security and complies with the University's requirements for handling any University data. Users are responsible for ensuring their use of OneDrive does not contradict any local or external requirements for storing or processing data (such as agreements with funding bodies or external data providers). **Please check with the Data Controller if OneDrive for Business is suitable for the data you wish to process.**

Ensuring that your working practices comply with the advice above will ensure your data remains safely and securely stored; that it cannot be accessed should your device be lost or stolen; and that any personal data is shared appropriately.

Whilst OneDrive for Business provides significant storage space (5TB) and convenience, **it is important to note that it is not a replacement for existing University or College approved file store platforms that you may already be using, for example SharePoint, departmental or College shared drives etc**. Long-term file-storage for College work should not take place on OneDrive. Please refer to the policy of your faculty, department or college with regards to the final storage location of any documents (including research materials).

By default, access to all your OneDrive for Business documents is restricted to you.

You can grant permission or full administrative rights to share files and folders with others within and without the University. You are responsible for managing the permissions for your documents. We strongly recommend that you consider carefully who you give administrative rights to as they can delete or reshare your documents without asking you.

To comply with the GDPR, personal data should be shared only with those who have a strict need to know. Please refer to College GDPR guidance for further information.

If, despite the availability of OneDrive for Business, you continue to store University data using other cloud-based services that do not comply with security or data protection requirements, you will be in breach of the data security advice exposing yourself and the University to unnecessary and potentially costly legal risk.

For further advice, please contact the College DPO.

USE ON COMPUTERS OR DEVICES YOU ARE USING TO ACCESS ONEDRIVE

- Ensure virus/malware detection software is installed with the latest definitions. The University provides Sophos for use on personal devices. Computers provided by the College will have such software installed.
- Do not log into your workstation or device as an administrator (unless absolutely necessary) even on your home computer.
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- **For support staff, or those who perform a College role, don't sync files to a machine or device that is not issued and secured by the college.**

BEST PRACTICES FOR SHARING FILES

- **OneDrive does not replace the College shared folders currently in place. It is strictly prohibited to store (rather than temporarily copy for editing) files from departmental shares on OneDrive.**
- Use folders to share groups of files with others online.

- Share files with specific individuals, never with “everyone” or the “public”.
- Review your use of sharing regularly.
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
- Remember that once a file is shared with someone and they download it to their device, they can share it with others.
- Remove individuals when they no longer require access to files or folders. This is your responsibility, and not that of the ICT Department.

UNCLASSIFIED DATA

Unclassified data may be stored and shared in OneDrive, but must be stored and shared in a secure manner.

Data that does not meet the criteria as Highly Protected or Protected as defined above shall be considered non-classified data. Please note that this classification does not imply that the data does not need to be properly managed. Such data may be subject to data subject requests.

WHERE CAN I PROCESS AND /OR STORE DATA (EXTERNAL CLOUD STORAGE SERVICES)?

	Dropbox Free version	Google Drive	iCloud
Process University or College data?	No	No	No
Storage available	2GB	15GB	5GB
Backup	Deleted items are held in the recycle bin for 30 days. Previous versions of files are available for 30 days.	Deleted items are held in the recycle bin for 30 days. Previous versions of files are available for 30 days.	Deleted items are held in the recycle bin for 30 days. Previous versions of files are available for 30 days.
Data location	Worldwide	Worldwide	Worldwide
File sharing possibilities (not an indication of whether or not to be used)	Anyone	Anyone	Anyone
Support	Dropbox	Google	Apple
Data access/ Account expiry	Perpetual unless account removed by owner.	Perpetual unless account removed by owner.	Perpetual unless account removed by owner.

DOCUMENT CHANGE LOG

Version	Date changed	Notes
1.0	16/05/2018	Version 1.0 published