Neil Favager
IT University of Leeds
22 February 2019

Information Management Guide

Essential before deciding where and how to store your information

The sensitivity of all information and data you create or receive must be assessed, classified and managed in accordance with the University Information Protection Policy. See Annex A for guidance.

Approved Storage Locations

The University has certain approved onsite storage and cloud rules. Currently the only fully supported cloud storage within the University are the options within Office 365, which all have the ability to synchronise with the device you are using.

Location	Non-classified	Confidential	Highly Confidential
M drive	Yes	Yes	Yes
N drive	Yes	Yes	Only if encrypted
One Drive	Yes	Yes	Only if encrypted and not synced locally.
SharePoint	Yes	Yes	Only if encrypted and not synced locally.
Microsoft Teams	Yes	Yes	Only if encrypted and not synced locally. Or Multi Factor Authentication is enabled.
University-owned laptops or other portable devices.		Only on a temporary basis and only if encrypted	Only on a temporary basis and only if encrypted. Only the absolute minimum data must be held in this manner.
Privately-owned laptops and tablets		No	No
External memory devices (i.e. memory sticks, Dictaphones, phones, cameras)		Only if no other option, device must be encrypted, remove ASAP	Only if no other option, device and data must be encrypted, remove ASAP
Sending data by e-mail internal (Outlook)	Yes	Yes	Yes good practice is to encrypt the attachment / email
Sending data by e-mail external	Yes	Yes (taking care to check the address of the recipient(s))	Yes but only as encrypted attachment

Table 1.1 University Policy with regards to cloud storage and mobile devices.

Information Storage on Microsoft Office 365

Office 365 offers an alternative location to storing your data on the traditional M or N Drives. This includes data that is also stored automatically within your Outlook mailbox. Office 365 offers more flexibility and storage capacity. It does however need to be managed appropriately. It has a higher potential for user error to accidentally share restricted information. The fundamental difference is that your data is not stored locally on University servers but is stored in the Cloud that is supported by servers offsite.

OneDrive what is it?

OneDrive for Business is a personal file store area available to all members of the University for the duration of your studies or employment. To get started with this Knowledge Base article KB0012306 can be found on the IT webpages. Each OneDrive account comes with 5TB of space.

OneDrive is perfect for these types of files:

- Those that you only want for you. Files that shouldn't or don't need to be shared.
- Drafts of files you're not yet ready to move to a SharePoint library or Team for collaborative input or reviews.

It is strongly discouraged to collaborate in OneDrive

Local synchronisation settings

You can synchronise copies of files in **OneDrive for Business** to your local device for use when you don't have an internet connection.

- Unclassified – full sync
- Classified – University Managed Devices – Permitted if documents are encrypted
- Classified – Devices not Managed by the University – Local sync is not permitted
- Encryption settings

Knowledge Base article KB0012504 explains how to do this.

Default sharing settings must be checked

How to change the default sharing link settings for OneDrive and SharePoint can be found in Knowledge Base article KB0012861 on the IT web pages.

SharePoint what is it?

SharePoint sites are created upon request by IT via the IT Service Desk. SharePoint is a team file store area designed to allow multiple access. It allow permissions to be granted on a site basis, instead of on individual documents. If people have access to the team site, then they have access to documents stored in the site. Then within the site it is possible to create further access permissions to particular folder areas.

Reasons to use SharePoint

- You want to create several areas of publishing information (such as a series of HR guidelines with a main landing page and supporting subpages)
- You want a site with specific configurations
- You want integration between sites and rollup of information
- Strict Governance, consistency, and structure are very important

It allows a team, service, school, faculty or project to plan to share files and with a limited scope or lifecycle. SharePoint can spread ownership and permissions across a wider collection of people. If a document or folder is important, it's a good idea for there to be a small number of people who can control what happens on the site as owners/administrators. To compare with One Drive see Knowledge Base article KB0012922.

Microsoft Teams what is it?

A local hub for teams to communicate and collaborate. It serves as a home for dedicated content. It is not typically used for organization-wide communication. Microsoft Teams build on the foundation of Groups as a "chat-based workplace," where all communication (whether in Skype, email, text, etc.) happens within that team. It includes a shared mailbox specific for that team.

Reasons to use Teams:

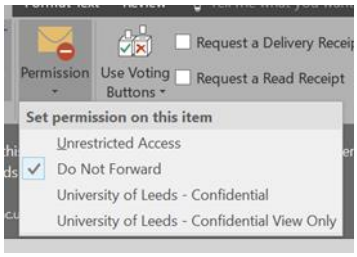
- You need to communicate with teams and individuals quickly
- You want to communicate, create tasks and share files with a specific group of individuals
- You're dealing with documents that are only pertinent to that group of individuals
- The communication you're having between team members tends to be less formal and has to be in a timely fashion
- If the group membership is small, ad-hoc, or fluid
- Teams has the ability to share the team's collaboration space with users from outside your organisation

More information on Teams can be found on the Knowledge Base Article KB0012997.

Outlook and your emails

The university Information Protection Policy allows for highly confidential emails to be shared following the guidance in the table 1.1. Your Outlook mailbox will automatically synchronise with your computer. This is also the case when accessing through the app or web. As a result to ensure compliance with the University Information Protection Policy all highly confidential emails should be immediately saved to an appropriate area and deleted from your mailbox.

Outlook also provides various other methods of protecting your messages that are simple to use. If you are sending an internal email, consider using the permissions tab. This controls what the recipient can do with your email and can even prevent a screen grab being carried out. This function can be found as shown in the graphic.



Options for full encryption of the message and attachments are the use of Word and Excel passwords or the 7zip function. More information can be found in the Knowledge Base article Email security KB0012279 and Sharing information securely KB0012620

Further proactive practices for confidential information within your mailbox should be to:

- Delete emails (and saved attachments) no longer needed – for staff and student data please follow the agreed retention policies.

  When deleting emails remember also to delete from the "Deleted Items" email folder too.

- Managing emails - for emails that need to be saved, it is a good idea to organise them into subfolders. This will make their management much easier. Put some time aside on a regular basis to review your subfolders, specifically to delete those e-mails that you no longer require.

Still have more Questions?

Knowledge Base article KB0012330 on the IT webpages provides a list of FAQ's

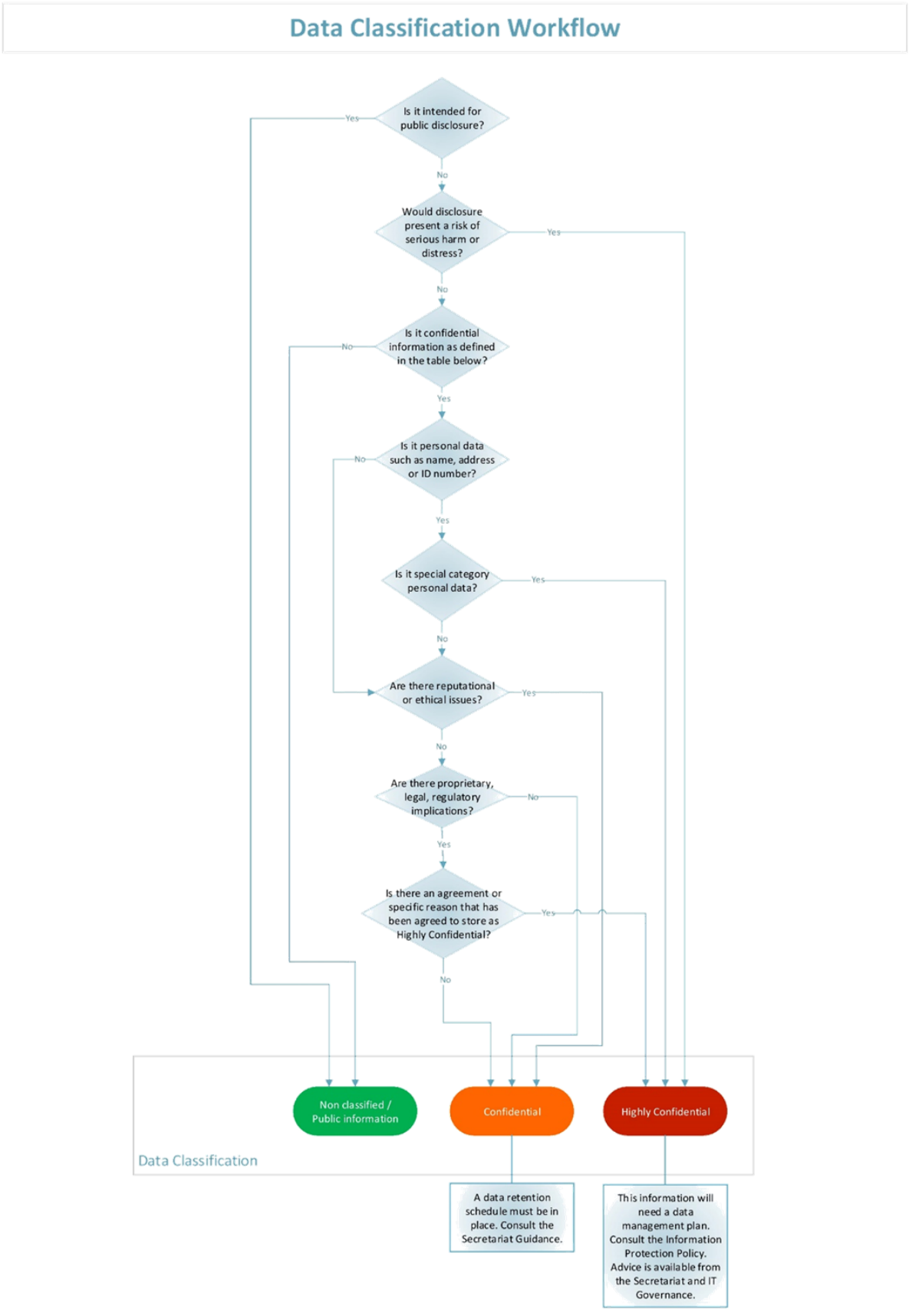
Protecting your device

More information on protecting your portable device can be found in Knowledge Base article KB0011076.

More information on Data Protection and Retention Schedules

You should delete all information, including emails, which contain personal data beyond the period defined in the Records Retention Schedule as keeping this is unlawful. Failure to do so may result in the University receiving penalties under the General Data Protection Regulations (GDPR). More information on data protection and retention schedules can be found on the University's data protection website

Annex A – Data Classification example



Personal Data		
Unclassified	**Classified / Confidential**	**Classified / Highly Confidential**
▪ Anonymised Data ▪ Data agreed by data subjects to be put into the public domain ▪ Publicly available staff directories including work telephone numbers, e-mail address and Department information ▪ Simple list of names with no other data. ▪ Information on individuals available through social network sites where information is provided on condition that it will be publicly visible. ▪ Final degree classification	▪ Individual's passport details, home address and telephone number. ▪ Individual's name plus home address/postcode, age and home telephone numbers. ▪ List of student names and their student ID number or list of staff names and their personnel number. ▪ Names and addresses of student applicants to the University. ▪ Attendance details relating to an existing student. ▪ Student transcript. ▪ Exam scripts. ▪ Exam marks. ▪ Examiner's comments on a student's performance.	▪ Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees). ▪ Information on individual's racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, genetics, biometrics, physical or mental health, sex life, sexual orientation or criminal record. ▪ Attendance and academic progression information/ disciplinary information relating to an existing University student. ▪ Preliminary degree classification/ transcript information pending formal approval and any publication.
References for students or staff		
▪ Dates of birth	▪ UCAS forms ▪ Individual's name plus date of birth or national insurance number	▪ Individual's name plus date of birth or national insurance number, passport details, home address and telephone number ▪ Hundreds of individuals' names plus date of birth or national insurance number

Non-personal Data		
Unclassified	**Classified / Confidential**	**Classified / Highly Confidential**
▪ Information contained within an organisation's annual corporate report. ▪ Information that can be obtained from publicly available directories or regulatory bodies e.g. Companies House or HEFCE. ▪ Information contained within an organisation's web sites for public dissemination.	▪ Research grant applications/proposals ▪ Information relating to the supply or procurement of goods/services prior to approval of publication. ▪ Assessment material prior to "unseen" assessment.	▪ Future marketing or student fees information not yet agreed to be made public. Other information that may be regarded as a trade secret or otherwise highly commercially sensitive. ▪ Information relating to restricted intellectual property rights or otherwise covered by a confidentiality agreement/ contractual term. ▪ Legal advice and other information relating to legal action against or by the University.