How to securely create, store and collaborate on Examination Papers

Please distribute the advice below within your institution. Full guidance on risks while working online can be found on https://help.uis.cam.ac.uk/service/security.

Below you can find more general guidance on the creation and storage of examination papers written with the expert help of the University's Central Exams Office. However we strongly recommend that you work through the steps in the Information Security Risk Assessment (ISRA) for full guidance https://help.uis.cam.ac.uk/service/security/for-it-staff/isra.

Step 1 Classify your Data

The University defines 4 levels for classifying data based on the impact that compromise of this data would have.

Data classification levels:

Level 3: High or Very High Impact

- There is a pressing requirement to limit who has access to it
- There is need to define who is on the access list
- There is a need to ensure that the above list is complete and doesn't just include people because of the nature of their jobs e.g. systems administrators (requiring a higher degree the need to know principal)

Level 2: Medium Impact

- Confidential information
- Information that may be dealt with by any staff with delegated responsibility from the recipient
- Restricted access is required but system administrators and super users can also have access

Level 1: Low Impact

- Data that is not quite public or publicised data and is required as part of people's jobs e.g:
  - Photoboard with job titles
  - Telephone list in a department
  - Lecture list with lecturer names and room details

Level 0: Negligible Impact

- All data that doesn't fall into one of the classifications above

Although examination papers are likely to be considered at the higher end of this scale ultimately it is down to an individual judgement based on local factors and, as recommended, the completion of an Information Security Risk Assessment.

> **Data requiring a higher degree of the 'need to know' principle**
>
> This covers data which you consider is highly confidential in that you wish this data to be only seen by designated people and not by some who may normally have access by the nature of their jobs (for example, not by HR staff or not by institution systems administrators).

Further information on the classification and handling of data can be found Reducing the Information Security Risk webpage.

Step 2 Perform Risk Assessment

As this information specifically relates to examination papers we have provided some general guidance in Step 3 but for completeness we recommend that you carry out an Information Security Risk Assessment (ISRA). Completing the ISRA could help you to:

- identify risks to your dataset
- highlight issues that prompt you to put new mitigating controls into place
- flag risks with transferring data between yourself and another institution
- provide evidence of good data management practice - for example, with respect to compliance with GDPR

> **Risk Assessment tip**
>
> The ISRA1 form asks you to consider all of your datasets. As we are specifically talking about examination papers you can skip straight to ISRA2 where you can consider the specific risks and threats.

Step 3 Reduce the Risk

Data handling

The initial preparation, editing and copying of examination papers needs to be undertaken under strict confidentiality.

The UIS Cyber Security Team together with the Examination and Assessment Committee recommend the use of Microsoft Teams or one of the cloud-based storage options - Microsoft OneDrive for Business, Google Drive or Dropbox for Business - for sharing examination papers within faculties and departments with the following considerations.

Microsoft Teams

The owners of the relevant Teams and Channels understand and accept responsibility for managing owners, members and guests. Further details on how your information in Teams is protected can be found Microsoft Teams at Cambridge Hub webpages.

> **Important note**
>
> Using MS Teams is also possible but the owner of that data should satisfy themselves that they have full and ongoing control over who can join the relevant team, and that they are comfortable with the possibility that platform administrators have an ability to access the data (See MS Teams security).

Microsoft OneDrive for Business / Google Drive / Dropbox for Business

Clear and transparent access management should be in place and someone has responsibility for checking access to make sure that requests for new access and access removal are dealt with quickly and efficiently.

> **Important note**
>
> Your cloud solution (e.g.OneDrive) replicates to any workstation or laptop you read these files on, and most files and documents have an auto-save or document recovery feature which creates temporary files on your device, so you may wish to put measures in place to either stop the replication or restrict the viewing of these files. To this end, it is recommended that your laptop has robust full disk encryption (e.g. Windows 10 bitlocker, MacOS Filevault or dm-crypt) and you don't read your work files or documents on your home device or anyone else's desktop/laptop without fully restricting such replication or saving.

A helpful comparison of the three tools can be found on Data Storage webpages.

Further information on the cloud storage options:

- OneDrive
- Google Drive
- Dropbox

Further helpful advice and considerations

- For added security on MS Teams and OneDrive, you could encrypt specific files which you do not want platform administrators to see. To do this, use the *Protect* function in Word, Powerpoint and Excel, for example, using a strong and long password, but remember to give the password to the recipients in a safe manner (e.g. via a separate device, or perhaps by voice in a meeting in MS Teams) and kee p it safe yourself (e.g. in a password manager).
- There are a few Office365 (OneDrive, MS Teams) administrators in UIS, who would technically have access, although these administrators have to follow the Charter for system and network administrators.
- Encourage colleagues involved in creation of the examination papers to process these paperless to avoid situations when papers are left unattended on a printer.
- When using Departmental shared drives, speak to your IT colleagues to ensure it is clear who has access to these.
- Encourage colleagues not to put examination papers on the USB devices especially if not password protected.
- Make yourself familiar with additional guidance on the Further Reducing the Risk webpages.