Delete unnecessary files

Information has become valuable and therefore special attention must be paid to the storage and processing of information. Proactive action can reduce data risks, such as data loss or leakage.

There is a wide variety of valuable information. It makes sense to consider which data loss or leakage would do the most damage to Metropolia. The risk of losing data can be reduced by backing up your most important files to multiple places. The risk of data leakage can be reduced by deleting unnecessary files from your computer and saving the files to a secure storage location and managing user permissions.

Important information may be:

- Passwords and usernames
- Project / project materials
- Health and other private information
- Financial information
- Files that contain a lot of information or work
- Thesis materials

1. How do I securely delete unnecessary files from my computer's hard drive?

Staff: See section 3. If your computer's Bitlocker protection is turned on, you can securely delete files normally by moving the files to the Recycle Bin and then emptying it.

Students and other stakeholders: See section 7.

2. Email mailbox

The e-mail inbox is not intended to be used for storing information, and therefore old unnecessary e-mails should be deleted from time to time. In particular, unnecessary e-mails that contain confidential or sensitive information must be removed from the e-mail. This will reduce the risk of data leakage.

https://oma.metropolia.fi/ Tools Common tools The Outlook / e-mail menu gives you access to your personal e-mail online, allowing you to see all the messages you have received in e-mail (even many years ago). After deleting emails, be sure to empty your mail trash bin.

2.1 Shared Mailbox

Talk to your team about who is responsible for maintaining a shared mailbox and how long emails should be kept. It is recommended that you create a document or annual clock in which this information is written.

2.2 Saving an Email as a File

In Outlook, it is possible to save an e-mail as a file on your own computer, for example in PDF format. This can be used, for example, to archive an important e-mail message. See the link below for instructions.

https://support.microsoft.com/en-us/office/save-saving-file-4821bcd4-7687-4d6d-a486-b89a291a56e2

3. Check that the Bitlocker protection is enabled

Bitlocker is a feature of the Windows operating system developed by Microsoft that encrypts your computer's hard disk. When it's enabled the hard drive cannot be accessed without the Bitlocker recovery key.

Bitlocker protection is enabled when there is a opened padlock on C drive (as shown below) when you open this PC menu . When encryption is enabled, files on your computer can be deleted normally by moving the files to the Recycle Bin and then emptying the Recycle Bin. If you don't already have Bitlocker protection on your computer, you can contact the helpdesk. If there is an error triangle on drive C, try restarting your computer once.

blocked URL

4. Erasing data from external storage device

Even if the external storage device is formatted (a function that deletes all files on the device), it is possible to recover old files until the device is overwritten. In projects where classified material has been processed on external storage devices, it is recommended to overwrite it. For overwriting, a separate program must be used. In other words, the program deletes the files and overwrites it with zeros and ones, so that the original files can no longer be restored. Open source overwrite software includes e.g. Eraser and WipeFile.

If you need to dispose external storage device, you can take it to the nearest helpdesk. Be sure to mention if classified data has been processed on your device so that helpdesk can take the necessary action.

5. Printing material and disposing physical documentation

When printing confidential or classified material, the following must be taken into account:

- Printouts containing such information cannot be left visible to others.
- When printing, retrieve the printouts immediately from the printer, so that you do not forget or confuse the printouts with others.
- All confidential and classified physical material must be placed in secure trash. For example, materials related to students course performance is always confidential information.

Printing of material and disposal of papers and other material

Action	Public information	Internal or limited use information	Confidential information	Classified information	Note
Printing of materials	Allowed	Allowed	Allowed	Allowed	
Paper material disposal, normal trash bin	Allowed	Not Allowed	Not Allowed	Not Allowed	
Paper material disposal secure trash bin	Allowed	Allowed	Allowed	Allowed	All confidential material is placed in the secure trash. Material related to course assignments is always confidential information.

CDs containing destructive material and other media, such as external recorders, can be delivered to your local Helpdesk.

6. Material management in RDI projects

Responsible material management is an important part of the RDI project. Well-managed material is reliable and can be relied upon in the conclusions of research or development. It is important to plan how and where the material will be stored and possibly disposed before the beginning of the project.

Check out the data management model (in Finnish) on the RDI support services website.

https://libguides.metropolia.fi/hankepalvelut/aineistonhallinta

7. Student - How do I delete my thesis materials securely?

Unnecessary material files and temporary files created in connection with the completion of the thesis must be deleted when the need for them ends. Simply deleting a file and emptying your computer's recycle bin does not mean that the file has been permanently destroyed. Deleted data can be recovered even after reformatting the hard disk. This is important to consider, especially if you plan to sell your old computer. There are various ways to destroy data securely, for example overwriting data or magnetizing the hard disk. Open source overwrite software includes e.g. Eraser and WipeFile. Overwrite programs can also be used to erase an external storage device.

Physical documentations that contain confidential or classified information must be placed in secure trash.

Hävitä tarpeettomat tiedostot