# Data and document protection

Every day we work with data — study materials, personal data of students, or internal documents of the faculty.
It is important to remember that data has value and must be handled safely – just like physical documents.

How to work with data safely
**Store documents in secure locations** – e.g. university cloud (Microsoft 365, OneDrive, SharePoint) or faculty storage.
**Do not use unverified services** such as unknown repositories, public sharing links, or personal drives without security.
**Consider who you are sending the data to**. If they are not intended for the public, do not send them outside the university environment.
**Do not store sensitive documents on USB flash drives without encryption.**

Document sharing
Only share with people **who really need to see them**.
In tools like **OneDrive or SharePoint, set a "Read-only" access** if the recipient does not need to edit the content.
**Do not send sensitive documents by email as attachments**. Instead, use sharing via the university cloud.
**Remove redundant accesses** after the end of the project or semester.

Working with personal data
If you are working with data from students, colleagues or research participants, make sure you follow the GDPR privacy policy .
Only store what you really need.
Do not work with personal data on public computers.
Do not transfer personal data tables outside the university.

Backup
**Back up important documents** – ideally to the university cloud or faculty server.
Never have a single copy of data on a laptop or flash drive only.

Remember
Working safely with data is everyone's responsibility.
Even one inadvertently shared file can cause sensitive information leak.

Frequently Asked Questions (FAQ)
**Can I use a private/personal cloud for university documents?**
- No, it may conflict with GDPR. Use only official university cloud services.

**Is it OK to send internal documents by email?**
- Only if they do not contain sensitive data. For more secure sharing, use the link to a file in the university cloud with restricted access.

**I lost my USB drive with my work files - what to do?**
- The loss must be reported to the faculty IT support or CSIRT-CUNI security team for evaluation of whether it classifies as sensitive data leak.

How to protect your data in 5 points
**Do not email** sensitive files without encryption.

**Store** data only on secure CU storage sites.
**Back up** important documents.

**Share** only with people who really need the data.
**Delete or restrict access** after the project is over.