Secure use of cloud services

For the purposes of these guidelines, cloud services refer to the cloud services used by Metropolia, which are Google Workspace for Education (e.g. Google Drive and Google Meet). & Microsoft Office 365 Education (e.g. Microsoft OneDrive, SharePoint, Teams and Stream). Each cloud service includes several applications in the product family to which the same guidelines for storing and processing data apply.

1. What data or information can be stored in the cloud?

Familiarize yourself with Metropolia's terms of use for cloud services, which specify in more detail what you can and cannot store in the cloud.

In addition to the terms of the cloud services, confidential information such as,

- Exam answers and other tests, including all kinds of assignments and examinations. However, grades and scores are public, meaning they can be stored in the cloud.
- Sensitive personal information, which includes;
- Information on the verbal assessment of a student's personal characteristics
- Information on the person's state of health, disability, health care or social care clientele or rehabilitation (e.g. applications and decisions on special arrangements for studies)
- Information concerning the person's annual income or total assets, or the income and assets on which the aid or benefit is based, or which otherwise describe his financial situation

Act on the Openness of Government Activities 24 § states what information and/or documents are classified information. In particular, teaching staff must take into account article 24 points 21, 22, 30, which are related to the documents to be processed in teaching. Among other things, the processing of information related to the thesis, research, development must be kept confidential so that it does not cause harm to the research or to the client. The same applies to information that would jeopardize the implementation of the test or exam. As well as documents related to the student such as a teaching waiver, test, certificate, or other documents that include a verbal assessment of personal characteristics.

Other administratively relevant 24 article points are 6, 7, 8, 11, 16, 17, 20, 23, 25. The owner / processor of the information is responsible for the classification of the information.

The data classification and secure storing table below is intended to clarify Metropolia's policy on the use of cloud services and in particular what may be published and stored in those applications / systems.

Data storage and processing in information systems and cloud services

Action	Public information	Internal or limited use information	Confidential information	Classified information	Note
Google products: Drive, Classroom, Blogger, Docs, Meet, Sites, Photos, Slides, Form	Allowed	Allowed	Allowed	Not Allowed	**Note!** Google product family includes several applications that are subject to the same data storage and processing guidelines as the listed services.
Microsoft 365 products: OneDrive, Onenote, Sites, Stream, Teams, Planner, Stream, Whiteboard, Sharepoint, Yammer	Allowed	Allowed	Allowed	Not Allowed	**Note!** Microsoft product family includes several applications that are subject to the same data storage and processing guidelines as the listed services.

2. Is all personal information classified information?

Not all personal information is directly classified information. For example, course attendance information and files containing student numbers can be stored in the cloud.

Special categories of personal data is always classified information. In Metropolia, sensitive personal information is usually health information. Particular attention is needed when handling sensitive personal information, as cyber criminals have found their high market value.

3. File sharing in cloud applications

When sharing files from Google or Microsoft cloud services, follow these rules. These rules must be followed without exception to ensure data security.

- When you share a file or folder with a Metropolitan (staff, student, stakeholders, etc.), use only his or her Metropolia cloud service account, not an external email address. Access to cloud services is available to every Metropolian. If you encounter a problem, do not resolve it by distributing material from the cloud services to an email address outside of Metropolia. In case of a problem contact the Helpdesk.
- When sharing a file or folder with a partner outside of Metropolia, use the email address of his or her own organization (workplace or school), not a gmail address or other personal email addresses.
- Do not share files or folders so that any link holder can access them (e.g. in Microsoft cloud services, do not select the option Anyone with the link but Specific people or People in Metropolia University of Applied Sciences Oy with the link)

- For Microsoft cloud services, use the "Expiration date" to determine the validity of the link

More information of cloud services.

4. Data protection - inquiries and remote interviews

- When conducting a survey, for example for a thesis or research, and the survey contains personal information, please note that it is recommended to use the E-form software to carry out the surveys. It is not recommended that queries be made on Google Forms or Microsoft Forms, as information about these is stored in the cloud service and may involve the transfer of personal data outside the EU/ETA, which is in principle problematic under data protection law.
- If you are conducting a remote interview that is to be recorded, please note that the use of the Zoom web conferencing tool is mandatory in this context. The Zoom recording does not go to the cloud storage, but by default the Zoom recording only goes to the local C network drive of the user's own computer. When recording with the Microsoft Teams Web Meeting Tool, the record goes to cloud by default. See the Zoom instructions here.

If you have any questions about using cloud services, send a message to ciso@metropolia.fi or helpdesk@metropolia.fi

Pilvipalveluiden tietoturvallinen käyttö