

Guidelines for the Use of Microsoft 365 by Employees at Mid Sweden University

Publicerad: 2026-08-25

Beslutsfattare: Avdelningschef, Helena Wallskog

Ansvarig funktion: Digitalisering och service

Handläggare: Sonja Balaz

Beslutsdatum: 2026-08-25

Giltighetstid: Tillsvdare

Senaste översyn: 2026-08-25

Sammanfattning: This document sets out guidelines for the use of Microsoft 365 at Mid Sweden University, with a focus on information management, security, storage, disposal, and the use of various services.

Tidigare versioner: MIUN 2020/740

Table of Contents

1. INTRODUCTION AND PURPOSE.....	3
2. REGULATIONS, CONFIDENTIALITY, AND PRIVACY	3
3. SENSITIVITY LABELS	4
4. RETENTION, DISPOSAL, AND STORAGE.....	4
4.1 <i>Retrospective Disposal</i>	4
5. GENERAL GUIDELINES FOR THE USE OF M365 AND COPILOT	5
6. SPECIFIC GUIDELINES FOR TEAMS AND SHAREPOINT	5
6.1 <i>Team Ownership and Responsibility</i>	5
6.2 <i>Naming</i>	5
6.3 <i>Chats</i>	6
6.4 <i>Channel Messages</i>	6
6.5 <i>Files in Teams and SharePoint</i>	6
6.6 <i>External Sharing</i>	6
6.7 <i>Meeting Recordings, Transcriptions, and Summaries</i>	6
7. SPECIFIC GUIDELINES FOR OUTLOOK	7
8. SPECIFIC GUIDELINES FOR ONEDRIVE.....	7
9. SPECIFIC GUIDELINES FOR FORMS	7
9.1 <i>Permitted Use</i>	8
9.2 <i>Personal Data and Information to Data Subjects</i>	8
9.3 <i>Responsibility for and Management of Responses</i>	8
9.4 <i>Disposal and Retention</i>	9
10. USE OF MICROSOFT COPILOT	9
10.1 <i>Restrictions on the Use of Copilot</i>	9
11. INCIDENTS AND MANAGEMENT OF NON-COMPLIANCE.....	9
12. RESPONSIBILITY	10
13. MONITORING AND FOLLOW-UP.....	10

Guidelines for the Use of Microsoft 365 by Employees at Mid Sweden University

1. Introduction and Purpose

Microsoft 365 (M365) is a cloud-based service provided by Microsoft that includes, among other applications, Outlook, Word, Excel, PowerPoint, Forms, OneDrive, SharePoint, Teams, and Copilot. The service is used for communication, collaboration, information storage, and information sharing within the University's operations.

Mid Sweden University shall manage information in M365 in accordance with applicable legislation and regulations, including the Freedom of the Press Act, the Public Access to Information and Secrecy Act, the General Data Protection Regulation (GDPR), and the University's own governing documents.

The purpose of these guidelines is to clarify how M365 shall be used in a manner that supports the University's operations, reduces risks, and ensures that information is managed in accordance with applicable laws, requirements, and internal procedures. The guidelines shall also assist employees in assessing what types of information may be handled in the various services.

These guidelines apply to all employees at Mid Sweden University who have access to M365. They replace the previous M365 regulations and clarify the University's shared approach to use, management, and responsibility. Following their adoption, the guidelines will be introduced through information on the employee webpages, targeted communication initiatives, and user support.

2. Regulations, Confidentiality, and Privacy

Mid Sweden University handles official documents while also being required to protect information subject to confidentiality. Consequently, information stored or shared in M365 must always be assessed on the basis of its content, purpose, and required level of protection.

The GDPR stipulates that personal data must not be processed to a greater extent or for a longer period than is necessary in relation to the purpose of the processing. Personal data in M365 should be deleted once the purpose of the processing has been fulfilled, provided that this is compatible with the applicable information management plan and disposal decisions (see [Archives and Records Registration](#)).

As M365 is an external cloud service, information subject to confidentiality or requiring special protection must be handled with great care. Confidential information, sensitive personal data, and information that is otherwise particularly worthy of protection must not be stored in M365.

Encryption shall be used for emails containing sensitive personal data, personal data requiring special protection, or confidential information, in accordance with the University's instructions (see [Procedures for Digital Workspaces for Employees at Mid Sweden University](#)).

3. Sensitivity Labels

Sensitivity labels are used to support the correct management of documents, emails, and other information in M365. The label indicates the applicable level of protection and helps users handle the information appropriately.

Labels shall be applied consistently and selected on the basis of the content of the information and its protection requirements.

Each employee is responsible for using sensitivity labels in accordance with the University's guidelines and selecting the appropriate label based on the nature of the information (see [Sensitivity Labels](#)).

4. Retention, Disposal, and Storage

M365 shall not be used for the long-term retention or archiving of records. Records that are to be retained shall instead be managed in the relevant business system or transferred to the University's archival function in accordance with established procedures (see [Email and Teams in Relation to Archival Requirements and the GDPR](#)).

Each employee is responsible for:

- reviewing and disposing of material in M365 workspaces in accordance with the information management plan and disposal decisions;
- transferring records that are to be retained to the appropriate business system; and
- avoiding the conversion of temporary workspaces into permanent storage locations.

4.1 Retrospective Disposal

To comply with applicable decisions, older emails and chats may be automatically disposed of in accordance with established procedures (disposal

decision 2022–2 and MIUN 2022/2745). The purpose is to remove information that should have been deleted earlier but remains stored.

5. General Guidelines for the Use of M365 and Copilot

M365 and its agents:

- must not contain confidential information, sensitive personal data, or personal data requiring special protection;
- must not be used for private purposes;
- must not be used in a manner that violates Swedish law, copyright, or the University's acceptable-use agreement;
- must not be used to offend, insult, humiliate, or harass others;
- may be installed on privately owned computers, but IT support is provided only for computers owned by Mid Sweden University; and
- may be used by each user on a maximum of five devices in accordance with the applicable licensing terms.

6. Specific Guidelines for Teams and SharePoint

Teams and SharePoint are used for collaboration, sharing, and joint work. The person who creates a team or group is responsible for ensuring that its content is managed in accordance with applicable regulations.

6.1 Team Ownership and Responsibility

- All groups and teams shall have at least two owners.
- The person who creates the team serves as the contact person for the Department of Digital Services (DOS).
- The owner is responsible for membership, access rights, naming conventions, and ensuring that the team remains current.
- The owner is responsible for removing teams that are no longer in use.
- Teams that have not been used for three months will be removed after the team owner has been notified. Automatic reminders will be sent to team owners.

6.2 Naming

Teams and groups shall be given clear and descriptive names that make their purpose readily understandable.

6.3 Chats

Chats in Teams shall be managed according to their content and context.

- Chats between employees within Mid Sweden University are, in most cases, not official documents.
- For such chats, the GDPR shall be taken into account, and the chats shall be reviewed or deleted when they are no longer needed.
- Chats between employees and external participants are generally official documents and shall be managed in accordance with the information management plan.
- Chats that need to be retained should be documented in an official memorandum before being disposed of in Teams.

6.4 Channel Messages

- Channel messages in internal teams are, in most cases, not official documents.
- For such messages, the GDPR shall be taken into account, and they shall be reviewed or deleted when they are no longer needed.
- Channel messages in external teams are generally official documents and shall be managed in accordance with the information management plan.
- Messages that are to be retained should be documented in an official memorandum before being disposed of in Teams.

6.5 Files in Teams and SharePoint

Files stored in teams and SharePoint may constitute either official documents or working material that does not qualify as an official document. Their content must therefore be assessed and managed in accordance with applicable regulations.

6.6 External Sharing

External sharing of files, folders, and workspaces in Teams, SharePoint, and OneDrive may take place only when justified by operational needs and in accordance with applicable information security regulations.

6.7 Meeting Recordings, Transcriptions, and Summaries

Meeting recordings, transcriptions, and automatically generated summaries shall be managed with the same care as other information in M365. The person responsible for the meeting shall assess whether recording or transcription is necessary and ensure that the material is managed in

accordance with applicable regulations and the information management plan.

Meeting recordings shall be disposed of two years after the meeting. For meetings involving external participants, retention may be appropriate if the recording is considered to have research value or has attracted significant public attention.

7. Specific Guidelines for Outlook

Outlook is used for email and calendar management. Emails shall be managed with the same care as other information.

- Outlook shall not be used as a long-term archive.
- Emails from external senders or addressed to external recipients are generally official documents and shall be managed in accordance with the information management plan.
- Emails sent to or received from external parties that do not constitute official documents shall be reviewed or deleted when they are no longer needed.
- Internal email correspondence between employees is, in many cases, not an official document and may be reviewed or deleted when it is no longer needed.
- For emails that are no longer needed, the GDPR principles of data minimisation and storage limitation shall be taken into account.

8. Specific Guidelines for OneDrive

OneDrive is a personal storage area for work-related files.

- OneDrive shall be used for files that are still in progress or that are not intended for long-term storage.
- OneDrive shall not be used as an archive.
- Records that are to be retained shall be transferred to the appropriate business system or submitted to the archives in accordance with established procedures.

9. Specific Guidelines for Forms

Forms is used for surveys, polls, and the straightforward collection of information.

The person who creates a form or survey is responsible for assessing how long the form, responses, and any compilations need to be retained. Once the purpose of the survey has been fulfilled, the form and associated results shall be deleted or disposed of in accordance with the applicable information

management plan, unless the material is to be retained in another system or transferred to the archives.

9.1 Permitted Use

Forms may be used for:

- straightforward surveys, evaluations, and registrations; and
- collecting information that is neither confidential nor sensitive.

Forms shall not be used for:

- processing sensitive personal data or confidential information;
- collecting information requiring a high level of protection; or
- situations in which specific requirements apply regarding secure storage, traceability, or long-term retention.

9.2 Personal Data and Information to Data Subjects

When collecting personal data, the person responsible for the form shall:

- ensure that the data subject receives clear information about how the data will be processed;
- collect only the data necessary for the stated purpose (data minimisation); and
- avoid free-text fields if there is a risk that sensitive information may be submitted.

Where standardised information text is required, it shall be provided in the form of a template or recommendation.

9.3 Responsibility for and Management of Responses

The person who creates a form is responsible for:

- defining the purpose of the collection and ensuring that the data is used accordingly;
- assessing how long the form and responses need to be retained;
- ensuring that only authorised persons have access to the responses; and
- exporting or transferring information to the appropriate business system when necessary.

9.4 Disposal and Retention

Forms shall not be used for long-term storage or archiving.

Once the purpose of the survey has been fulfilled:

- survey questions, responses, and compilations shall be managed—retained or disposed of—in accordance with the applicable information management plan; and
- information that is to be retained shall be transferred to the appropriate system or archival function.

10. Use of Microsoft Copilot

Employees at Mid Sweden University may use Microsoft Copilot in the areas of M365 where the service is available. Copilot is a generative AI tool that can be used to search for information, analyse material, create drafts, and improve texts.

When Copilot is used through the University's login, the same information-management requirements apply as for other M365 services. Users must therefore pay particular attention to the information entered in prompts.

10.1 Restrictions on the Use of Copilot

The following must not be entered into Copilot:

- personal data that clearly identifies an individual;
- material over which the user does not have the right to exercise unrestricted control; or
- other protected material that should not be shared through the service.

Employees are responsible for reviewing information generated by Copilot before using it further.

11. Incidents and Management of Non-Compliance

If an employee discovers or suspects that someone is violating these guidelines, the matter shall be handled as an incident in accordance with Mid Sweden University's incident-management process (MIUN 2026/1729).

The system owner or responsible function may shut down or remove groups and teams for operational-security reasons or where there are reasonable

grounds to suspect a violation of the University's acceptable-use agreement or internal regulations.

In the event of a violation, measures may also be taken in accordance with Mid Sweden University's acceptable-use agreement.

12. Responsibility

Each employee is responsible for complying with these guidelines, the University's acceptable-use agreement, and all other applicable procedures. Upon termination of employment, the employee is responsible for managing information and records in accordance with the applicable information management plan and, where necessary, ensuring that ownership of teams or other workspaces is transferred to another authorised person.

13. Monitoring and Follow-Up

M365 system management will continuously monitor compliance with these guidelines in the tools included in M365.