



BAU

BAHÇEŞEHİR
UNIVERSITY

MICROSOFT 365 COPILOT INSTITUTIONAL SECURITY AND EFFECTIVE USE GUIDE

*Guidance for increasing productivity in academic and administrative processes
while protecting institutional data, human responsibility, and trust*

Version	01
Publication Date	29 June 2026
Feedback and Contact	AI Competency Unit
Document Coordination	Information Technology Directorate and AI Competency Unit
Training and User Support	BAUPRO, Information Technology Directorate and AI Competency Unit

How to Use This Guide

This Guide explains the account, data, security, verification, and human-responsibility principles that apply when Microsoft 365 Copilot, Copilot Chat, and related Copilot features are used in education, research, work, projects, and institutional duties connected with Bahçeşehir University.

Five questions before using Copilot

1. Am I signed in with my institutional BAU account or my personal account?
2. Is the information I intend to use public, internal, personal, or confidential?
3. Do I have the necessary role-based authority and legal basis to process this information with Copilot?
4. Can I verify the output and take responsibility for it?
5. Does the use involve a meeting recording, institutional data source, Copilot agent, plugin, connector, or sharing with other users?

Additional assessment may be required

If the answer to the final question is “yes,” a technical, data-protection, or institutional assessment may be required before the feature is placed into use.

Quick Reference

Area of use	General approach
BAU institutional Microsoft 365 environment	BAU provides institutional Microsoft 365 accounts and services to faculty, staff, and students. This account does not automatically provide access to all advanced Copilot features.
Copilot Chat - institutional account	A conversational AI service available within the University's licensing and technical configuration. Functions may vary according to the user's licence and enabled features.
Personal account or individual subscription	Faculty, staff, and students may access Microsoft Copilot with personal Microsoft accounts or purchase individual subscriptions. This Guide still applies when used for BAU-related work; internal and confidential information must not be transferred to a personal account.
Advanced Microsoft 365 Copilot	Advanced use integrated with applications such as Word, Excel, PowerPoint, Outlook, and Teams may require an additional licence assignment and the necessary institutional assessment.
Public or low-risk content	May be used for drafting, summarisation, idea generation, language improvement, and general analysis. The output must be verified.
Internal or controlled content	Should be used only through the institutional account, for a role-related purpose, and within existing access permissions.
Personal, confidential, or restricted-access content	Use of an institutional account alone is not sufficient. A legal basis, role authority, data minimisation, and necessary institutional controls are required.
Official or people-impacting use	Must not be converted into a decision or action before human review and authorised approval are completed.

Core distinction

An institutional Microsoft 365 account is not the same as an advanced Microsoft 365 Copilot licence. The fact that a feature appears in the user interface does not mean that it is approved for every form of institutional use.

Contents

1. Purpose of the Guide.....	5
2. Scope.....	5
3. Institutional and Personal Access to Copilot.....	5
3.1. BAU Institutional Microsoft 365 Environment.....	5
3.2. Microsoft 365 Copilot Chat.....	5
3.3. Personal Accounts and Individual Subscriptions.....	6
3.4. BAU-Related Use through a Personal Account.....	6
4. Core Approach: Copilot Assists, Responsibility Remains Human.....	6
4.1. Purposeful and Proportionate Use.....	6
5. Privacy of Use Content and Technical Administration.....	6
5.1. BAU's Institutional Approach.....	6
5.2. Technical and Aggregate Usage Data.....	7
5.3. Exceptional Circumstances.....	7
6. Account, Access and Licence Use.....	7
6.1. Institutional Account.....	7
6.2. Personal Account.....	7
6.3. Advanced Microsoft 365 Copilot Licence.....	7
6.4. Access Review.....	8
7. How Copilot Works with Institutional Data.....	8
7.1. Existing Access Permissions.....	8
7.2. Enterprise Data Protection.....	8
7.3. Sensitivity of Combined Information.....	8
8. Secure Use Based on the Nature of Information.....	8
8.1. Common Data Rules.....	9
9. Effective Use Areas.....	9
9.1. Academic and Teaching Activities.....	9
9.2. Research and Scientific Production.....	9
9.3. Administrative and Institutional Activities.....	9
9.4. Accessibility and Language Support.....	10
10. Use Reminders Across Microsoft 365 Applications.....	10
11. Human Oversight, Verification and Quality Assurance.....	10
11.1. Disclosure of Copilot Use.....	11
12. Teams Meetings, Recording, Transcription and Summarisation.....	11
12.1. Before Use.....	11
12.2. Sensitive Meetings.....	11
12.3. Meeting Outputs.....	11
13. Copilot Agents, Plugins and Connectors.....	11
13.1. Before Creating an Agent.....	12
13.2. Core Rules.....	12

13.3. Sharing Agents.....	12
13.4. Plugins and Connectors.....	12
14. Records, Retention and Sharing.....	12
14.1. Before Sharing.....	12
15. Uses That Are Not Permitted.....	13
16. Error, Incident and Breach Reporting.....	13
Initial steps.....	13
17. Institutional Roles and Responsibilities.....	13
17.1. Users.....	13
17.2. Academic and Administrative Units.....	13
17.3. Information Technology Directorate.....	14
17.4. AI Competency Unit.....	14
17.5. BAUPRO.....	14
17.6. Office of Legal Counsel.....	14
18. Support and Training.....	14
19. Brief Checklist Before Use.....	14

Technical features, licensing, and user interfaces may change over time. Current announcements from the Information Technology Directorate and applicable Bahçeşehir University regulations govern institutional use.

1. Purpose of the Guide

Bahçeşehir University regards Microsoft 365 Copilot and Copilot Chat as productivity tools that support human capacity in academic, research, administrative, and institutional processes. The purpose of this Guide is to provide implementation guidance for the safe and effective use of Copilot services for the following purposes:

- Promoting safe and purpose-aligned use,
- Protecting institutional data and personal data,
- Maintaining human evaluation and ultimate responsibility,
- Verifying generated content, analyses, and recommendations,
- Managing accounts, access, sharing, and licences appropriately,
- Supporting proportionate and efficient use in education, research, and administrative processes.

This Guide shall be applied together with the Bahçeşehir University Artificial Intelligence Policy, the Responsible Artificial Intelligence Implementation Procedures and Principles, the Artificial Intelligence Use Guide for Faculty and Staff, the Artificial Intelligence Use Guide for Students, the Personal Data Protection and Data Privacy Policy, and other University regulations concerning information security, intellectual and industrial property, academic integrity, and records management.

2. Scope

This Guide applies, to the extent that access to the relevant service or feature is provided, to:

- Faculty members,
- Administrative staff,
- Academic and administrative managers,
- Researchers,
- Undergraduate and graduate students,
- Authorised persons carrying out projects or services on behalf of the University.

The Guide applies to the following services and areas of use:

- Microsoft 365 Copilot Chat,
- Microsoft 365 Copilot,
- Copilot functions in Word, Excel, PowerPoint, Outlook, Teams, OneDrive, SharePoint, OneNote, and Loop,
- Copilot agents,
- Plugins, connectors, and external data connections associated with Microsoft 365 Copilot,
- Related Copilot features subsequently introduced by Microsoft and enabled by the University.

This Guide applies to Copilot use connected with education, research, work, projects, services, and institutional duties at Bahçeşehir University, regardless of whether access is through an institutional account or licence provided by the University or through the user's personal account and individual subscription.

Use entirely for personal purposes and unrelated to the University is outside the institutional workflow.

Nevertheless, obligations concerning personal data protection, information security, intellectual property rights, and professional responsibilities continue to apply.

3. Institutional and Personal Access to Copilot

3.1. BAU Institutional Microsoft 365 Environment

Bahçeşehir University provides institutional Microsoft 365 accounts and services to its faculty, staff, and students. Word, Excel, PowerPoint, Outlook, Teams, OneDrive, SharePoint, OneNote, and other Microsoft 365 applications form part of the University's institutional digital working and learning environment.

Possession of an institutional Microsoft 365 account does not automatically provide access to all advanced Microsoft 365 Copilot features or functions that require an additional licence. Available Copilot features may vary according to the licences held by the University, the licence assigned to the user, and technical configurations implemented by the Information Technology Directorate.

3.2. Microsoft 365 Copilot Chat

Microsoft 365 Copilot Chat is a conversational artificial intelligence service that eligible users may access through their institutional work or school accounts within the University's licensing and technical configuration. Copilot Chat's capacity to work with web content, institutional files, agents, or other work data depends on the user's licence, access permissions, and features enabled by the University.

3.3. Personal Accounts and Individual Subscriptions

Faculty, staff, and students may access Microsoft Copilot through personal Microsoft accounts or purchase eligible individual Microsoft 365 subscriptions using their own resources and use Copilot features intended for personal use.

A personal Microsoft account and the institutional work or school account provided by BAU are separate account and service environments. Purchasing an individual subscription does not convert the account into an account provided or approved by BAU for institutional use.

3.4. BAU-Related Use through a Personal Account

Carrying out BAU-related work through a personal account or individual subscription does not remove the user's responsibilities arising from University regulations. Personal accounts may be used for low-risk BAU-related tasks only with information that is:

- Publicly available,
- Free of personal data,
- Not confidential or subject to restricted access,
- Not subject to contractual, licensing, or intellectual-property restrictions.

An individual subscription does not grant institutional authority

Paying for a personal subscription does not authorise a user to transfer BAU internal files, personal data, confidential information, or restricted-access content to a personal account.

4. Core Approach: Copilot Assists, Responsibility Remains Human

Copilot may be used for idea generation, drafting, structuring information, simplifying text, improving language and expression, summarisation, table and data analysis, presentation preparation, task planning, research support, and facilitating repetitive tasks.

However, Copilot does not replace:

- Academic or professional expertise,
- Human judgement,
- Scientific responsibility,
- The authorised decision-maker,
- Institutional approval, authority, and signature responsibility.

The user must be able to understand, question, verify, modify, or reject Copilot output.

Responsibility cannot be delegated

The fact that content was prepared by Copilot does not remove the academic, administrative, legal, or institutional responsibility of the person who uses, shares, approves, or converts it into a decision.

4.1. Purposeful and Proportionate Use

Copilot should be used when it makes a genuine contribution to the nature of the task. Users should avoid unnecessarily repeating the same request, engaging in long and purposeless conversations that create no value, or transferring tasks to AI when they can be completed more simply by another method.

Purposeful and targeted use supports more efficient use of time, computing resources, and institutional capacity.

5. Privacy of Use Content and Technical Administration

5.1. BAU's Institutional Approach

During ordinary use and routine institutional administration, Bahçeşehir University does not examine, at content level, users' individual prompts, conversations, files, drafts, working methods, or generated text, analyses, or code in Copilot; nor does it assess employee performance or student achievement on the basis of such content.

Work content is not a performance measure

Individual Copilot conversations, prompts, and work content are not used for performance or achievement assessment during ordinary institutional administration.

5.2. Technical and Aggregate Usage Data

For the purposes of managing institutional licences, security, resources, and service continuity, the following types of technical or aggregate information may be monitored:

- Whether an account or licence is active,
- Whether use occurred within a particular period,
- Total or group-level usage indicators,
- Licence and resource use,
- The name, owner, and access status of institutional agents that have been created or shared,
- Security or inappropriate-use alerts,
- Technical errors and service interruptions.

These data may be used for licence planning, user support, identifying training needs, information security, and service sustainability.

5.3. Exceptional Circumstances

In exceptional circumstances involving a legal obligation, information-security incident, authorised institutional review, official investigation, or the user's explicit request and permission, necessary action shall be carried out only through authorised processes and to the extent required.

BAU's institutional content-privacy approach does not provide the same institutional assurance for personal Microsoft accounts and individual subscriptions purchased by users. The service provider's personal-use, retention, and privacy terms apply to those accounts.

6. Account, Access and Licence Use

6.1. Institutional Account

When internal information, institutional documents, or Microsoft 365 content are used for BAU duties, the institutional Microsoft 365 account provided by the University must be used.

Users must not:

- Transfer institutional information to personal Microsoft accounts,
- Move institutional files to personal cloud accounts,
- Sign in on behalf of another person,
- Share account or authentication information.

Shared user accounts, common sessions, or use of Copilot on behalf of another user are not permitted.

6.2. Personal Account

Personal Microsoft accounts and individual subscriptions may be used for BAU-related low-risk tasks only with public information that does not require protection. Internal, personal, confidential, or restricted-access content must not be transferred to a personal account.

6.3. Advanced Microsoft 365 Copilot Licence

Use of advanced Copilot features based on institutional work data in Word, Excel, PowerPoint, Outlook, Teams, and other Microsoft 365 applications may require the assignment of an appropriate Microsoft 365 Copilot licence to the user.

Requests for advanced licences are evaluated with regard to:

- The nature of the role and the operational need,
- Expected area of use and institutional benefit,
- Licence capacity and budget,
- Information-security and data requirements,
- Required training and user readiness.

Technical licence assignment, account, and authorisation operations are carried out by the Information Technology Directorate. The AI Competency Unit contributes to assessing the use need and responsible-use conditions.

6.4. Access Review

Access or a licence may be reviewed in the following circumstances:

- The relationship with the University ends,
- A role or duty changes,
- The licence is no longer required,
- Prolonged inactivity,
- An information-security risk,
- The relevant feature is discontinued by the University,
- Required training or conditions of use are not completed.

7. How Copilot Works with Institutional Data

7.1. Existing Access Permissions

Microsoft 365 Copilot may draw upon content that the user is authorised to access in the Microsoft 365 environment. It does not create a new access right to documents or data for which the user lacks permission.

It does not correct existing permissions

Copilot does not automatically correct existing access permissions that were granted incorrectly or too broadly. A document shared improperly may become easier to surface in Copilot responses for users who already have access to it.

Users should therefore:

- Check file and folder sharing permissions,
- Use “Everyone” or broad-group links only when genuinely necessary,
- Verify recipients and access groups for sensitive documents,
- Ensure access is updated when duties change.

7.2. Enterprise Data Protection

Prompts, responses, and authorised institutional data used through Microsoft 365 Copilot and Copilot Chat with an institutional account are subject to Microsoft’s enterprise data-protection provisions. Under Microsoft’s enterprise commitments, these data are not used to train the underlying artificial intelligence models.

Before using Copilot, users should verify that they are signed in with the correct BAU account and that the interface displays the indicator confirming enterprise data protection is active. If this indicator is absent, personal, internal, or confidential information must not be entered and technical support should be requested.

7.3. Sensitivity of Combined Information

Copilot may combine information from multiple documents or sources. Information that is low or medium sensitivity when viewed separately may produce a more sensitive result when combined.

Copilot output should therefore be assessed not only by the nature of each source, but also by the new meaning, access implications, and confidentiality risk created by combining them.

8. Secure Use Based on the Nature of Information

This is not a new classification system

This section does not create a new or independent official information-classification system for the University. It applies the data-protection and risk approach adopted in the Artificial Intelligence Use Guides for Faculty and Staff and for Students to Microsoft Copilot use. More detailed provisions in applicable University information-security or classification regulations shall also apply.

Nature of information	Examples	Copilot use approach
Public or low-risk information	Published web content, public legislation and reports, general drafts that contain no personal data, anonymous or synthetic examples	May be used with an institutional account. It may also be used with a personal account; output must be verified and copyright, licence, and course rules observed.
Internal or controlled information	Routine internal correspondence, unpublished administrative drafts, non-sensitive course materials, general meeting notes, unit working documents	Should be used only through the BAU institutional Microsoft 365 account, for a role-related purpose, and within existing access permissions. It must not be transferred to personal accounts.
Personal, confidential, or restricted-access information	Student and employee information, health and special-category data, financial records, HR and disciplinary documents, legal files, unadministered assessment material, confidential research and invention information, confidential third-party content	Use of an institutional account alone is insufficient. It must not be used without a legal basis, role authority, purpose limitation, data minimisation, and necessary institutional controls.
Security information	Passwords, multi-factor authentication codes, API keys, access tokens, private keys	Must not be entered into any Copilot prompt, whether through an institutional or personal account.

8.1. Common Data Rules

- Use only the minimum amount of data necessary for the task.
- Remove personal identifiers where possible.
- Prefer anonymous or synthetic examples.
- Use only the necessary part of a document rather than the entire document.
- Check your authority to share and process the information.
- Review the conditions governing licensed or confidential third-party content.

Internal does not automatically mean suitable for Copilot

Also assess whether the information is necessary for your duty, whether you are authorised to use it, which account is open, and with whom the output will be shared.

9. Effective Use Areas

9.1. Academic and Teaching Activities

- Preparing draft course materials and activities,
- Developing sample questions and synthetic cases,
- Generating activity ideas aligned with learning outcomes,
- Structuring content from public sources,
- Preparing presentation and visualisation drafts,
- Developing a draft structure for student feedback.

Student personal data, final examination questions that have not yet been administered, answer keys, and protected question banks must not be used without the necessary controls.

9.2. Research and Scientific Production

- Developing research questions and search terms,
- Structuring the literature,
- Creating code and analysis drafts,
- Considering methodological and visualisation options,
- Preparing project or funding-application drafts,
- Improving language and expression,

- Drafting a response to reviewers.

Sources, citations, methods, calculations, and scientific claims must be verified against primary sources. Confidential peer-review documents, unregistered invention information, and unauthorised research data must not be used.

9.3. Administrative and Institutional Activities

- Preparing correspondence, report, email, and announcement drafts,
- Creating meeting agendas and action lists,
- Summarising public or authorised information,
- Preparing checklists and process drafts,
- Creating presentations and tables,
- Drafting responses to frequently asked questions,
- Classifying and analysing low-risk data.

Content prepared by Copilot must not be used as an official letter, institutional opinion, decision, instruction, or commitment before it has undergone authorised human review.

9.4. Accessibility and Language Support

Copilot may be used for plain language, summaries, alternative explanations, improved text structure, and translation drafts involving low-risk content. Legal, health-related, security-critical, reputationally significant, or official translations must not rely solely on Copilot output and must undergo competent human review.

10. Use Reminders Across Microsoft 365 Applications

Bahçeşehir University provides institutional Microsoft 365 services and accounts to its faculty, staff, and students. Possession of a Microsoft 365 licence does not automatically provide access to all Copilot features.

The availability of Copilot Chat, Copilot features within applications, responses grounded in institutional data, Teams meeting summaries, advanced agents, and other functions may vary according to the user's licence and the University's technical configuration. Features requiring an additional licence or approval are not deemed institutionally authorised merely because they appear in the user interface.

Application or service	Effective use	Special point of attention
Copilot Chat - institutional account	Idea generation, drafting, web research, and, to the extent permitted by the licence, work with files or work data	Confirm that the BAU account is open and enterprise data protection is active. Remember that features vary by licence.
Microsoft Copilot - personal account	Personal or low-risk support using public information	Do not use BAU internal, personal, confidential, or restricted-access content. An individual subscription does not provide institutional authorisation.
Word	Drafting, summarisation, restructuring, improving expression	Verify sources, persons, dates, obligations, and official wording.
Excel	Draft formulas, table analysis, trend and visualisation suggestions	Test formulas, data ranges, missing values, and calculations.
PowerPoint	Presentation structure, slide drafts, visual ideas, speaking notes	Check institutional identity, accuracy, accessibility, and image rights.
Outlook	Email drafts, subject lines, summaries, response preparation	Check recipients, attachments, commitments, dates, and confidential information before sending.
Teams	Meeting preparation, transcription in appropriate meetings, action items	Assess participant notification, authority to record, confidentiality, and retention rules.
OneDrive and SharePoint	Working with authorised documents	Check sharing permissions, anonymous links, former-user access, and the data owner.
Image generation	Conceptual images, presentation drafts, teaching materials	Do not portray a real person or event misleadingly; do not present an image as evidence or an official record.

11. Human Oversight, Verification and Quality Assurance

Copilot may generate non-existent sources, misrepresent an existing source, provide outdated information, make numerical or logical errors, misunderstand the context of a file, produce biased output, and present incorrect information in convincing language.

The user must therefore:

1. Verify critical claims against reliable and primary sources.
2. Check that sources, legislation, publications, and links actually exist.
3. Test numerical results, formulas, code, and analyses.
4. Use current and authoritative BAU sources for institutional information.
5. Check dates, persons, duties, authority, amounts, and institutional commitments.
6. Assess whether output creates bias, discrimination, or exclusion risk.
7. Revise the final text for its purpose, audience, and institutional context.
8. Where necessary, record verification steps in important or high-impact work.

Fluent text is not a guarantee of accuracy

The fact that Copilot produces fluent, professional, and convincing text does not mean that the content is accurate, current, or institutionally approved.

11.1. Disclosure of Copilot Use

Low-level use, such as spelling correction, simplification, or idea generation, does not need to be separately disclosed in every case. Copilot use should nevertheless be disclosed appropriately when:

- It has contributed to a significant part of an academic or scientific output,
- It has played a determining role in generating analysis, methods, code, or interpretation,
- It has produced a substantial part of public or institutionally significant content,
- It has been used in a decision-support process affecting people,
- The relevant course, publisher, funder, or institutional process requires disclosure,
- It would be misleading to create the impression that the content was produced entirely by a person.

12. Teams Meetings, Recording, Transcription and Summarisation

Use of Copilot, recording, or transcription features in Teams meetings must be assessed according to the nature of the meeting.

12.1. Before Use

- Participants must be clearly informed.
- It must be assessed whether the meeting is suitable for recording or transcription.
- The purpose of the use must be defined.
- Personal-data and retention conditions must be checked.
- Where participants from outside BAU are present, contractual and confidentiality obligations must also be assessed.

12.2. Sensitive Meetings

Unless specific authorisation or legal review has been obtained, recording, transcription, or Copilot summarisation should not be used in meetings concerning:

- Health and psychological-counselling information,
- Disciplinary processes,
- Human-resources and performance evaluations,
- Sensitive student-specific assessments,
- Legal advice and litigation strategies,
- Discussions covered by attorney-client confidentiality,
- Unregistered inventions or confidential research information,
- Third-party information protected by contract,
- Security incidents and sensitive system configurations.

12.3. Meeting Outputs

A meeting summary produced by Copilot does not replace official minutes. It may misrepresent participants' views, attribute decisions and tasks to the wrong persons, or produce incomplete results. It must be reviewed by the person responsible for the meeting before being used as an official or institutional record.

13. Copilot Agents, Plugins and Connectors

Copilot agents may be created to use particular information sources, support tasks, or facilitate workflows. The fact that an agent has been created does not mean that it is institutionally approved or may be shared throughout the University.

13.1. Before Creating an Agent

- Purpose and scope of use,
- Institutional owner, responsible person, and alternate responsible person,
- Data and information sources,
- Target user group and access level,
- Human oversight, known limitations, and risks,
- Update frequency and feedback channel,
- Conditions for retirement.

13.2. Core Rules

Copilot agents:

- Must not make final decisions affecting people independently.
- Must not be configured to initiate unauthorised actions.
- Must not be built with instructions containing passwords, access keys, or personal identity information.
- Must not be connected to institutional resources unrelated to their purpose.
- Must not be shared with restricted-access sources without the data owner's knowledge and necessary assessment.
- Must not conceal known limitations from users.

13.3. Sharing Agents

- Users' access permissions to the sources used by the agent must be verified.
- Where restricted-access sources are used, the data or content owner's view must be obtained.
- Unnecessarily broad user groups must not be selected.
- The agent's purpose and limitations must be explained to users.
- Access groups must be reviewed periodically.

Removing access to an agent or connector may not automatically remove pre-existing access to related files and folders. File and source permissions must be managed separately.

13.4. Plugins and Connectors

Plugins and connectors linking Copilot to external data sources or services must not be enabled for institutional use before they have been assessed by the Information Technology Directorate for technical and security purposes; where necessary, by the Office of Legal Counsel for contractual and data-protection purposes; and by the unit owning the use case for purpose and data-source suitability.

Incorrectly configured connector permissions may make sensitive content visible to a wider audience than intended.

14. Records, Retention and Sharing

Copilot conversations and temporary outputs must not be used as the sole storage location for important institutional records.

A Copilot output should be saved in the appropriate institutional document or records environment when it:

- Affects a decision-making process,
- Forms part of official correspondence,
- Has continuing institutional value,
- Constitutes evidence for a project, research activity, or administrative process.

Saved content must be managed with the appropriate access level, shared only with authorised persons, subject to the University's retention and disposal rules, and archived or removed when it is no longer current.

14.1. Before Sharing

- Check recipients' access authority.
- Verify the scope of the file link.
- Assess whether documents used by Copilot contain more sensitive information.
- Check whether combining multiple sources has created a new confidentiality risk.
- Remove unnecessary recipients, attachments, and links.

15. Uses That Are Not Permitted

The following uses are not permitted:

- Delegating final decisions with significant effects on students, employees, or third parties to Copilot,
- Using Copilot output as an official or academic output without verification,
- Generating fabricated data, sources, citations, evidence, minutes, or records,
- Processing personal or confidential information without the necessary authority and legal basis,
- Entering a password, access key, or security token into a prompt,
- Attempting to bypass information-security controls or access permissions,
- Transferring BAU information to personal accounts or unapproved external tools,
- Using another person's work or licensed content contrary to the rights holder's conditions,
- Generating content that misleadingly impersonates real people or events,
- Misleadingly presenting AI-generated content as entirely human-produced,
- Using a Copilot agent outside its approved purpose,
- Sharing an agent that uses institutional data with unauthorised or unnecessarily broad user groups,
- Reducing human oversight to a merely formal approval.

16. Error, Incident and Breach Reporting

The relevant institutional channel must be notified when any of the following occurs:

- Personal or confidential information is entered into Copilot accidentally,
- A file or agent is shared with unauthorised persons,
- There is suspicion that an institutional account has been compromised,
- An agent or connector is misconfigured,
- Copilot unexpectedly surfaces sensitive content,
- A serious, discriminatory, or harmful output may create institutional impact,
- An attempt is made to bypass a security control,
- A personal-data breach is suspected.

Initial steps

1. Stop the relevant operation.
2. Where possible, remove the sharing link or restrict access.
3. Preserve available records such as files, links, screenshots, and time information.
4. Inform the relevant unit manager and the Information Technology Directorate.
5. Where personal data are involved, ensure that the University's data-breach and legal-assessment process is initiated.

The AI Competency Unit contributes to assessing the incident in terms of the AI use case, user guidance, and necessary improvement.

17. Institutional Roles and Responsibilities

17.1. Users

- Use the appropriate account for institutional duties.
- Comply with this Guide and related University regulations.
- Check the data and access permissions.
- Verify Copilot output.
- Assume ultimate responsibility.
- Report incidents and errors without delay.

- Complete required training.

17.2. Academic and Administrative Units

- Assess the need for Copilot use and the expected institutional benefit.
- Relate licence requests to roles and needs.
- Identify ownership of their data and content sources.
- Assign responsibility for agents developed by the unit.
- Monitor access, updates, and retirement processes.

17.3. Information Technology Directorate (BIDB)

- Carries out account, licence, and technical-access operations.
- Manages Microsoft 365 administrative configurations.
- Applies authentication, access, and security controls.
- Performs technical assessments of agents, plugins, and connectors.
- Monitors technical use, service continuity, and security indicators.
- Responds to information-security incidents.
- Provides technical support to users.

17.4. AI Competency Unit

- Provides guidance on institutional use cases and responsible use.
- Coordinates development of the Guide and support materials.
- Contributes to evaluating licence requests in terms of purpose and institutional benefit.
- Collects user feedback and good practices.
- Contributes to the development of the purpose, ownership, and human-oversight approach for institutional agents.
- Provides monitoring and evaluation information to the Artificial Intelligence Steering Committee.

17.5. BAUPRO

- Prepares and delivers Microsoft 365 Copilot training content.
- Develops training pathways according to role and area of use.
- Maintains training participation and completion records.
- Updates training content with contributions from the Information Technology Directorate and the AI Competency Unit.

17.6. Office of Legal Counsel

- Provides advice on personal-data protection, contracts, intellectual property rights, and legal risks.
- Contributes, where necessary, to the legal assessment of agents, connectors, and data-use scenarios.
- Coordinates with relevant institutional units in legal incidents and breach processes.

18. Support and Training

Users may benefit from University training and support in the following areas:

- Use of Copilot Chat,
- Copilot in Microsoft 365 applications,
- Effective prompt writing,
- Institutional data security,
- Academic and research use,
- Administrative productivity,
- Teams meeting features,
- Creating Copilot agents,
- Output verification,
- Incident and error reporting.

Users assigned an advanced Microsoft 365 Copilot licence are expected to complete the basic training specified by the University. Training may be defined as a prerequisite for particular features or high-impact use cases.

For a new, uncertain, or high-impact use case, the relevant academic or administrative manager, the Information Technology Directorate, the AI Competency Unit, and, where necessary, the Office of Legal Counsel should be consulted before the feature is placed directly into use.

19. Brief Checklist Before Use

- ☐ I checked whether my institutional BAU account or personal account is open.
- ☐ If I am using a personal account, I am using only public and low-risk information.
- ☐ I checked whether my institutional Microsoft 365 account includes the relevant advanced Copilot licence.
- ☐ I understand that the appearance of a feature in the interface does not mean it is approved for institutional use.
- ☐ I confirmed that enterprise data protection is active.
- ☐ I assessed the nature of the information I will use.
- ☐ I have the role authority and necessary legal basis to process the data.
- ☐ I am using only the minimum amount of data necessary.
- ☐ I have not shared a password, access key, or security token.
- ☐ I checked the sharing permissions of files and sources.
- ☐ I considered whether Copilot could produce a more sensitive result by combining multiple sources.
- ☐ I will verify the accuracy, currency, sources, and calculations of the output.
- ☐ Ultimate human evaluation and responsibility remain with me or the authorised decision-maker.
- ☐ If I use meeting recording or transcription, I have informed the participants.
- ☐ If I use an agent or connector, its purpose, owner, sources, and user group are defined.
- ☐ I checked that the people with whom I will share the output are authorised.
- ☐ I assessed whether the use needs to be disclosed.
- ☐ I know which channel to use if an error or security incident occurs.

Final check

If you cannot confirm any of these items, make the necessary correction before continuing or seek advice from the relevant institutional support channel.

USE COPILOT • PROTECT DATA • VERIFY • TAKE RESPONSIBILITY