**8 Responsible use practices**

You are expected to understand and follow these 8 practices:

1. Avoid unethical prompting
2. Use in Teams meetings appropriately
3. Avoid using Copilot for private purposes
4. Confirm use in client engagements
5. Use sensitivity labels & check permissions
6. Avoid untested live demos
7. Check for accuracy and bias
8. Be transparent

# 1.  Avoid unethical prompting

You should not submit prompts that may lead to harmful, biased, or misleading content.

Avoid prompts that:

* evaluate the behavior or performance of an individual or group
* identify sentiment, and/or emotions of any individual
* refer to protected groups (e.g. gender, ethnic groups)
* ask about illegal or unethical matters
* ask that third-party content be incorporated into the output
* include references like “based on” or “in the style” of  particular authors or works
* edit or create images about other individuals

# 2. Use in Teams meetings appropriately

**Do not use in meetings involving:**

* Matters related to someone's sensitive personal data or private information (e.g., health, political beliefs)
* Corporate investigations, litigation or disputes.
* Other legal or compliance topics (unless requested by an Avanade legal counsel in the meeting).
* HR processes or procedures about a specific person or group, (e.g., performance evaluations).
* Candidate interviews.
* Client matters and data not approved by Avanade account Senior Leadership (ACAL or equivalent).
* Small groups like 1:1 meetings unless between Executives only.

# 3. Avoid using Copilot for private purposes

Since Copilot for M365 queries information within our corporate M365 applications, Avanade or client data may be automatically pulled into a response.

You may only use Copilot for limited private purposes if you can ensure Copilot is not using Avanade or client´s data when creating content.

Personally owned data should always be

* segregated from Avanade or client data
* stored within a single folder location for files and within a separate folder for emails

Any use outside of the conditions explained in this training may result in liability for you and or Avanade.

To prevent Copilot for M365 from sourcing your private files:

1. Create a folder to store personal files locally on your computer C drive:
   1. Start / File Explorer / Windows (C:) / New Folder

2.Name the folder ‘Private’

1. Files saved in this folder will not be backed up.

Remember that private files and emails on Avanade owned devices should be separate from Avanade and Client data.

# **4. Confirm use in client engagements**

**For Client engagements**, confirm with the Avanade account Senior Leadership (ACAL or equivalent) that Copilot for M365 is allowed to be used to process and or produce client-related work.

There may be contractual restrictions (e.g., restrictions on use of a particular technology or location of client data).

# 5. Use sensitivity labels & check permissions

Sensitivity labels may not automatically carry over from the source document, for example, if you copy an output from Copilot for M365 into another document.

**You must manually apply the applicable sensitivity label to the content you generate.**

Maintain sensitivity designations to comply with Avanade [Policy 1431AVA (Data Management)(opens in a new tab)](https://avanade.sharepoint.com/:f:/r/sites/Policies/Policies2/Data%20Management?d=wbe3ccc87476d4b5fb1bf790f98fe4dde&csf=1&web=1&e=0PLLew).

**See how to apply sensitivity labels to your content here:**[**Protect Data with Sensitivity Labels (sharepoint.com)(opens in a new tab)**](https://avanade.sharepoint.com/sites/ProtectAvanade2/SitePages/Microsoft-Purview-Information-Protection.aspx)

**Apply permissions** to restrict access to files and emails to those with a business need and restrict use of the file (e.g. edit vs view).

Before you share, ask yourself:

* Do I have permission to forward or share this information?
* Should I be sharing this information?

To prevent leakage of information, **check who has existing access to your files**.

1. Click on **Share**.

2. Select **Manage Access**.

3. **Remove**users, groups, or links that no longer require access.

**You can also do this from microsoft365.com. Go to “Shared” and  select “By you”**

# **6. Avoid untested live demos**

If demoing Copilot for M365, make sure to **first verify the content of documents, emails, or chats** that Copilot will query so you don’t inadvertently expose proprietary, (highly) confidential, or restricted information or personal data during the demo.

# 7. Check for accuracy and bias

**Look out for inaccurate information:**

* Ensure accuracy by asking Copilot for M365 to cite the sources it used; and/or directly reference the files you would like to use

**Be watchful for toxic and biased outputs:**

* Output must reflect our core values and comply with [Policy 1001 – Respecting the Individual(opens in a new tab)](https://avanade.sharepoint.com/sites/Policies/Policies2/Forms/AllItems.aspx?id=%2Fsites%2FPolicies%2FPolicies2%2FRespecting%20the%20Individual%2F1001%5FRespecting%5Fthe%5FIndividual%2Epdf&parent=%2Fsites%2FPolicies%2FPolicies2%2FRespecting%20the%20Individual). Be particularly vigilant if outputs concern protected groups (e.g. ethnicity, religion, gender identity).
* Report and discard toxic outputs.

Report any problematic content to copilot@avanade.com.

# 8. Be transparent

* Don't hide the use of Copilot. Failure to be transparent (particularly in meetings) could upset colleagues or clients and cause a loss of trust.
* Inform and allow people to object before turning on Copilot for M365 during a meeting (verbally or via the meeting chat).
* Label content created by Copilot for M365, if you didn´t materially change the output, so others are aware it was created with gen AI.

# **Before you start using Copilot for M365**

Get your information ready:

* •

Review sensitivity labels and whom you are sharing your files, Teams and SharePoint sites with.

* •

Delete old or unnecessary data.

* •

Obtain confirmation from the CAL to use Copilot for M365 for a client engagement.

* •

Store your private files on your Windows (C:) drive to avoid access from Copilot