

Working with AI, Safely

Copilot Chat (Basic) & M365 Copilot (Premium)

UBC IT · Microsoft 365 Phase 2 · All staff & faculty · 60 minutes

Trust Before Adoption



Same house, same locks

Copilot is a Microsoft 365 service inside UBC's enterprise tenant — behind the **same boundary that already protects your Teams, OneDrive, and Exchange.**

It sees only what you can already see
Copilot works within your existing permissions. If you can't open a file, neither can Copilot.

Your prompts don't train the models
Prompts, responses, and your data are not used to train the underlying foundation models.

UBC adds its own layer of locks
Privacy impact assessment, sensitivity labels, SharePoint indexing reviews, and UBC's AI Strategy Framework guardrails.

We won't just assert this today — we'll show you, live.

Where your data lives — and where it doesn't go

UBC'S MICROSOFT 365 SERVICE BOUNDARY

Exchange
email & calendar

Teams
chats & meetings

OneDrive
your files

SharePoint
team sites

Your data — governed by your permissions, CWL sign-in, and MFA

Copilot Chat · Basic

Does NOT read your UBC data. It sees only what you upload or paste into the chat — plus the web.

M365 Copilot · Premium

Grounded in your work — email, files, meetings — strictly within your existing permissions.

ENTERPRISE AI — both run in here. Prompts and responses stay inside the boundary; models store nothing and learn nothing from them.

The public web
Copilot can search it for current answers — with citations

CONSUMER AI
Personal ChatGPT, Gemini, Claude.ai accounts — outside the boundary, no enterprise promises. Never for UBC work.

What actually happens when you press Enter

1. You prompt

In plain language — a question, a task, a draft to improve

2. Grounding

Copilot adds context: the web, plus any files you hand it

3. The model reasons

Inside the service boundary; nothing is stored or learned

4. Checks & citations

Responsible-AI filters run; sources are attached

5. You get a draft

Into your chat history — which you control and can delete

The step that makes it “yours” is grounding.
A model on its own knows nothing about UBC. Grounding is what turns a generic answer into your answer — and it is permission-trimmed at every step: Copilot can only ground on content the signed-in person is allowed to open.

UBC’s added layer — what we did before saying “go”

Privacy impact assessment

Completed for Copilot in UBC’s environment before rollout — FIPPA obligations reviewed.

Sensitivity labels

Labels (Low → Very High) are now available in your Microsoft 365 apps so you can classify files by risk — you apply them; they travel with the file.

Data stewardship by design

Labels inform, people decide: no automated blocking at launch. Today’s labelling lays the foundation for future safeguards.

SharePoint indexing review

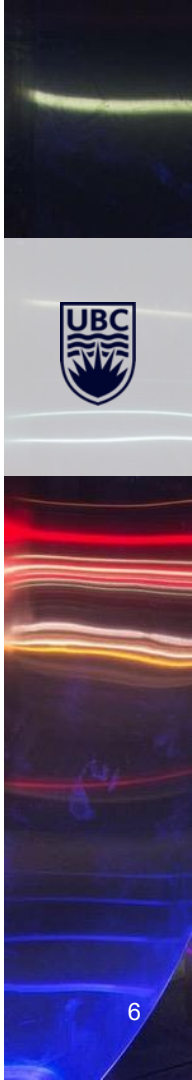
Site owners review whether their sites should be discoverable by Copilot before launch.

AI Strategy Framework

UBC-level guardrails governing responsible AI adoption across the university.

Managed onboarding

Premium is a managed, department-approved subscription — not an uncontrolled free-for-all.



Copilot grants no new access — it makes access visible

Copilot only ever sees what you can already open. But it finds and summarizes in seconds — so a file that is overshared today becomes **easier to stumble on tomorrow.**

Where oversharing hides

- A SharePoint site still includes people who left the project
- A folder shared with a whole department when a small team needs it
- An old sharing link that still works after its purpose ended
- A sensitive document copied into a less-restricted location
- A workspace with no clear owner reviewing membership

Your 5-minute review — start with one site you own

- What information is stored here — and who owns it?
- Does everyone with access still need it?
- Any external users or live sharing links?
- Is the sensitivity label correct for the most sensitive content?
- Should anything be moved, archived, or deleted?

Technical access ≠ legitimate business need. If Copilot surfaces something outside your role, don't explore it — tell the site owner so the sharing gets fixed.

The Copilot Ecosystem



Two Copilots, one rule: know which one you're in

	COPILOT CHAT · "BASIC"	M365 COPILOT · "PREMIUM"
What it costs you	Included for everyone with UBC M365	Paid add-on licence, via your department
What it knows	The web + files you upload in chat	Your work: emails, meetings, chats, files
Where it lives	Browser — m365copilot.com, Teams, Outlook	Browser + inside Word, Excel, PowerPoint, Outlook, Teams
Model access	OpenAI GPT models, standard priority	Priority access + Anthropic Claude (Opus, Sonnet) models
Extras	Pages, image generation, file upload	+ Notebooks, Create, Copilot Search, memory across work
Best at	Research, drafting, thinking out loud	Work grounded in your own content & workflows

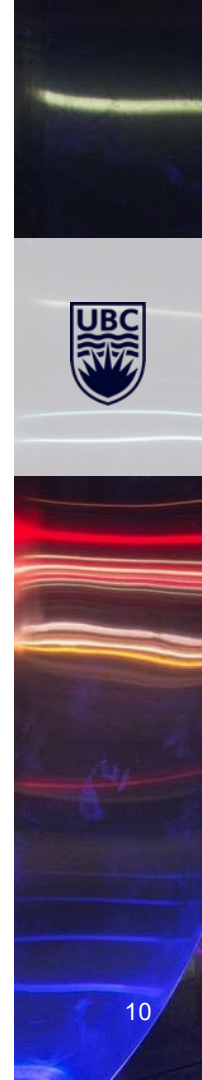
Where to find Copilot Chat (and how to know it’s the safe one)

m365copilot.com
The front door. Sign in with your CWL (UBC) account — this is today’s demo home.

Teams and Outlook
Copilot Chat appears in the app rail — same protected experience, beside your work.

Edge sidebar
Chat beside any webpage while you browse — handy for summarizing what you’re reading.

The green shield is your seatbelt.
Top-right of the chat window: a green shield means enterprise data protection is on— your prompts are protected, not used to train models. No shield? You’re in a consumer experience. Stop and sign in with your CWL.



What the included tier already does — no licence, no cost

Web-grounded answers

Current information from the live web, with citations to check

Work with your files

Upload documents into a chat: summarize, compare, extract, rewrite

Draft anything

Emails, outlines, reports, announcements — in your voice, iteratively

Generate images

Illustrations and visuals for slides, posters, and communications

Copilot Pages

Turn a good chat into a living, editable document you can share

Latest OpenAI models

GPT-5-class models with Auto / Quick / Think Deeper — standard priority (Claude is Premium-only)

Pick the right brain for the job

Quick response

Routine questions, quick drafts, simple rewrites

“Summarize this paragraph” · “Draft a two-line reply”

Think Deeper

Multi-step reasoning, analysis, weighing trade-offs

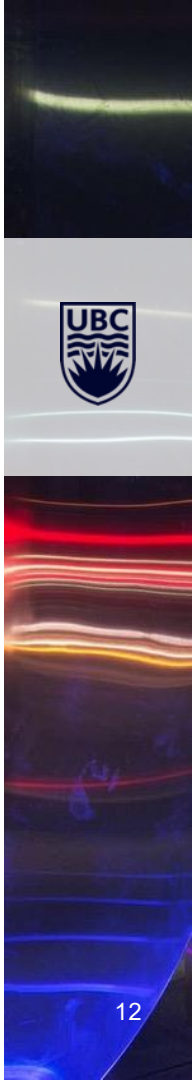
“Compare these three policy options and recommend one”

Auto (default)

Copilot routes each prompt to the best model for it

Fine for most work — override it when the task is critical

In Copilot Chat the selector runs on **OpenAI’s GPT models** — Anthropic’s Claude models (Opus, Sonnet) appear only with a Premium licence. Microsoft adds and swaps models regularly; the menu you see in the demo is this week’s, so learn the decision habit, not the model names.



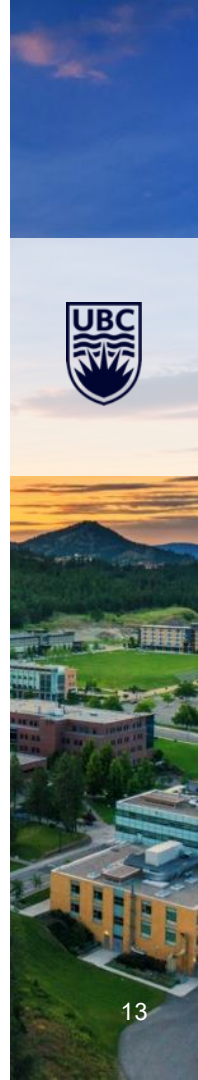
Make it yours — personalization that compounds

Custom instructions — teach it your role once
"I'm a finance clerk in UBC Facilities; keep answers concise; use Canadian spelling; format numbers as tables." Every future chat starts from there.

Memory — it remembers what matters
Copilot saves useful facts from your chats (and you can tell it: "remember that…"). View, edit, or delete every memory in Settings → Personalization.

Saved prompts — build your personal playbook
Save your best prompts in Prompt Gallery and share them with your team. UBC-curated prompts will appear right on the Copilot Chat home page and in Prompt Lab.

You stay in control
Every personalization feature has an off switch. Memory, instructions, and history are yours to review and clear at any time.



Working with AI, Responsibly



Verification discipline — the habit that makes AI safe

AI output is a **starting point**, never the final word. You sign your name to the result — so make it yours.

Check the citations

Every claim that matters gets a source check. No citation? Treat it as unverified.

Read before you send

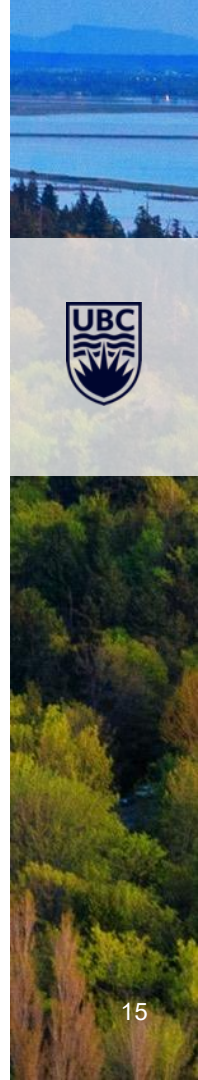
You are the author of record. Never forward AI text you haven't fully read.

Watch for confident nonsense

Models can be fluently wrong — especially with numbers, names, dates, and policy details.

Keep judgment human

Decisions about people — grades, hiring, funding — are made by people, informed by AI at most.



UBC sensitivity labels — know your document's risk

1 — Low Risk

Freely shareable; minimal harm if disclosed.

e.g. Staff contact info · public web content · published research · marketing materials

2 — Medium Risk

Could harm UBC if disclosed; share on a need-to-know basis.

e.g. Internal budgets · NDA-covered info · unpublished proprietary research

3 — High Risk

Legally protected (FIPPA) or regulated (PCI). Never share publicly.

e.g. Student IDs & grades · home addresses · HR records · credit card data

4 — Very High Risk

Significant harm if disclosed; data-steward approval, auditable sharing.

e.g. SIN · personal health information · biometrics · passwords & keys · government IDs

Mixed content? Label to the highest sensitivity present. Apply labels from the Sensitivity control in Word, Excel, PowerPoint, and Outlook. High and Very High ask you to pick a sub-label (Internal Only / External Sharing Allowed).

Labels + Copilot — three rules that keep you safe

Check the label before you bring a document to Copilot or using an output from Copilot

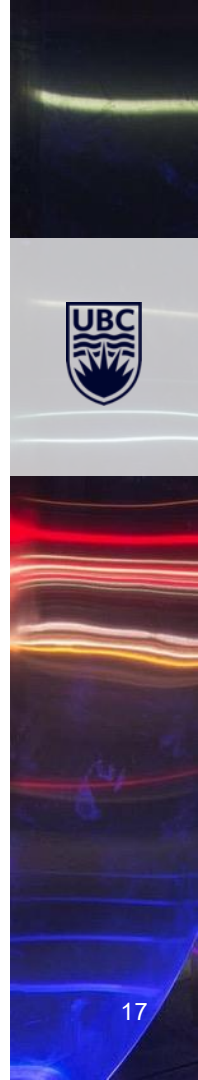
The label is your go/no-go. Low and Medium: work away. High or Very High: stop — confirm your use is appropriate and approved before Copilot touches it or before sharing the output

Copilot won’t block you — because you’re the data steward

No automated blocking at launch: if you can open a document, Copilot can work with it. The label tells you the risk; the decision — and the accountability — is yours.

Content Copilot generates inherits the label

Ask Copilot to draft from labelled sources and the output automatically carries the highest source label — protection follows the content.



Dos and don’ts — the UBC Copilot house rules

DO

- Sign in with your CWL account — confirm the green shield before working
- Check the sensitivity label and the permissions before bringing a document to Copilot
- Use Copilot only for a legitimate UBC purpose — and only the information that purpose needs
- Verify citations and read everything before you rely on it or send it
- Give context-rich prompts: goal, background, source, format
- Ask your supervisor or the accountable owner when the intended use is unclear

DON’T

- Don’t use personal / consumer AI accounts for UBC work
- Don’t feed it High or Very High Risk content without approval — or paste passwords, SINs, health or banking details
- Don’t let Copilot make, recommend, or influence decisions about individuals — hiring, discipline, admissions, academic standing
- Don’t use Copilot to collect information about identifiable people from the web
- Don’t explore content just because Copilot made it easy to find — report oversharing instead
- Don’t try to bypass a warning, restriction, label, or other safeguard

Prompting that works — give it what a good colleague would need

GOAL

What do you want, exactly?

“Draft a 200-word update for faculty…”

CONTEXT

Background, audience, constraints

“…about the lab move; audience is non-technical staff…”

SOURCE

What should it work from?

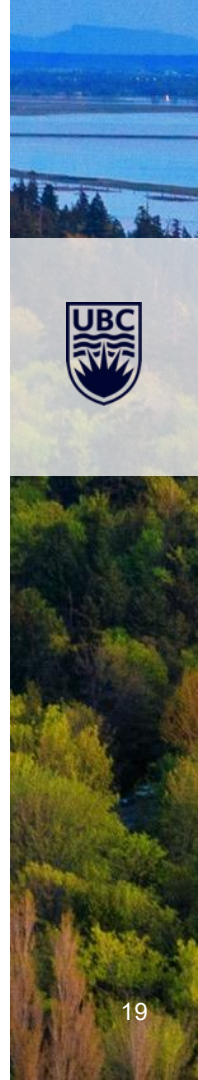
“…based on the attached project brief…”

FORMAT

Shape of the answer

“…as a friendly email with 3 bullets and a deadline.”

Then iterate. The first answer is a first draft — push back: “shorter”, “more formal”, “as a table”, “what did you miss?”. Treat it like a conversation with a capable new colleague, not a search box.

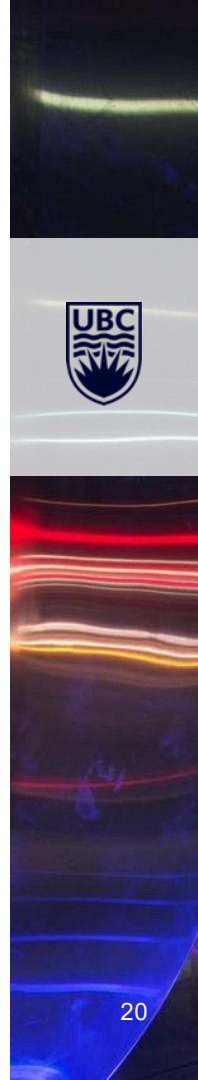


When a task outgrows the free tier

Copilot Chat can’t see your work content — so the moment a task depends on it, you’ve found a Premium use case. The signals:

“Catch me up on the emails I missed this week”	**Premium territory**
“Summarize yesterday’s project meeting and pull my action items”	**Premium territory**
“Draft the report directly in Word, from our last three updates”	**Premium territory**
“Find every document our team wrote about the budget review”	**Premium territory**

Recognize yourself here? Talk to your manager about the Premium cohort sessions — departments request licences through UBC IT’s managed subscription process.




UBC
THE UNIVERSITY OF BRITISH COLUMBIA