

AI: Information Governance, Copilot, and Your Responsibilities

Sensitivity labels rollout: what every UBC employee needs to know

UBC Information Technology | Abbreviated from UBC AI Foundations, Module Five



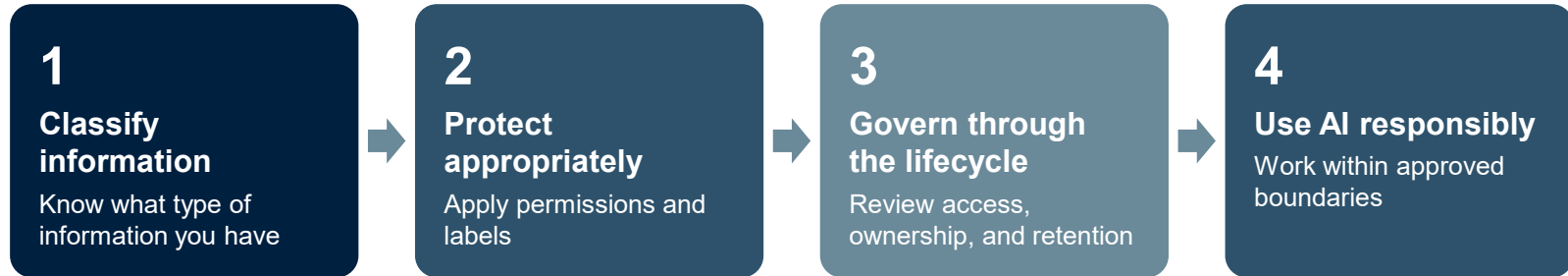
Why information governance matters for AI

UBC employees create, share, store, and use information every day. Some of it is public; some is sensitive and must be protected. A published paper and a student grade record need very different handling.

Information governance is how UBC organizes responsibility for information across its lifecycle: classification, access, privacy, security, records management, and responsible use.

AI raises the stakes. AI can find, summarize, and combine information quickly. If a file is overshared or its permissions are out of date, Copilot can make that already-accessible information easier to discover.

A simple information governance process for responsible AI



Not a one-time activity: information, access needs, and risk change over time, so labels and permissions should be reviewed regularly.



How information governance shapes sensitivity labels

Information Governance decides what information UBC holds, who is accountable for it, how sensitive it is, who should have access, and how it is managed over its lifecycle.

Sensitivity labels translate those decisions into a consistent, machine-readable classification that travels with information in Microsoft 365.

Implementing labels is not only a technology project. The label is the visible signal; the governance work behind it determines what the label means and how the information is protected.

What UBC needs first: people who understand and classify their information, confirm access is appropriate, and apply labels consistently. That creates the foundation for future protection and automated safeguards.

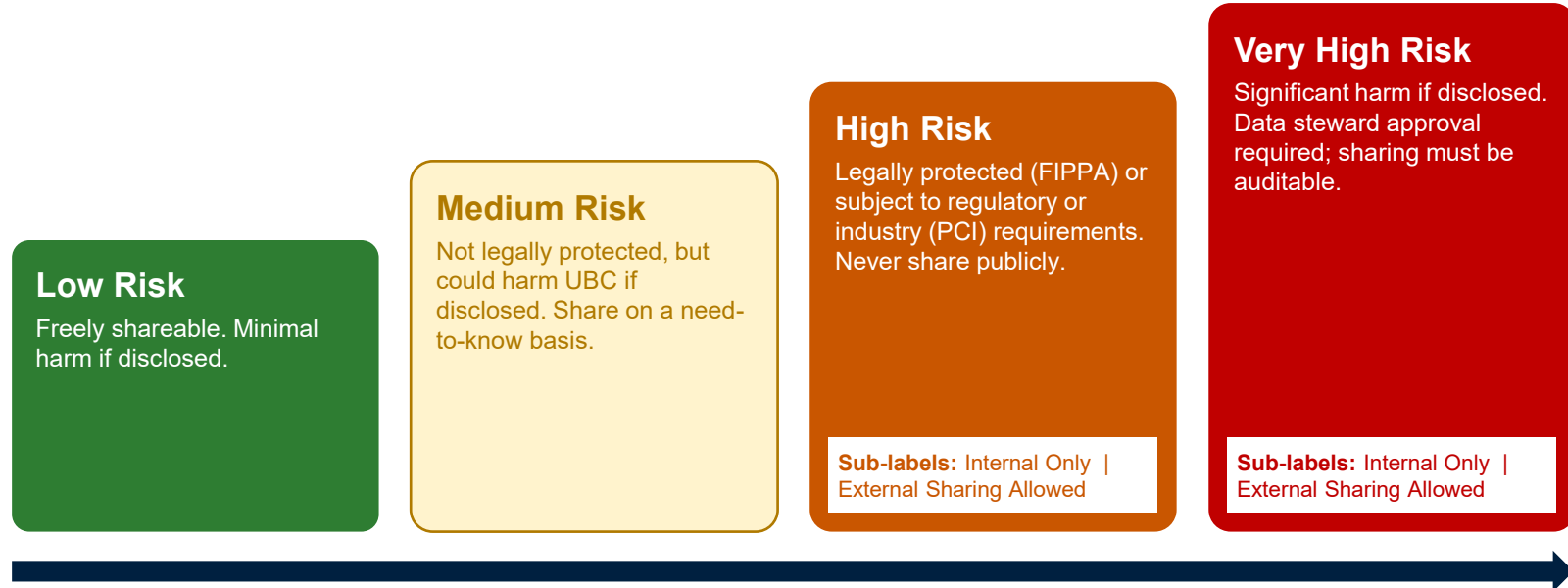
Information Governance contributes by defining:

- 1 A clear classification approach**
Aligned with the UBC Information Security Standard U1
- 2 Labels connected to requirements**
Privacy, security, records, research, contractual, and operational
- 3 Clear responsibilities**
Information owners, data stewards, content owners, and users
- 4 Oversharing addressed first**
Review permissions before stronger automated controls arrive
- 5 Guidance across the lifecycle**
Applying, reviewing, changing, and escalating labels



The four levels of UBC sensitivity labels

UBC's Microsoft 365 label framework is based on the UBC Information Security Standard U1 classification model. High Risk and Very High Risk include sub-labels for Internal Only and External Sharing Allowed.



Increasing sensitivity, potential harm, and handling requirements

Sensitivity labels: definitions and examples



Label	Definition and handling	Examples
Low Risk	Freely shareable. Minimal harm if disclosed.	Staff contact information; public website content; published research outputs; UBC marketing materials; public course syllabi
Medium Risk	Not legally protected but could harm UBC if disclosed. Share on a need-to-know basis.	NDA-covered information; restricted journals; confidential financial records and internal budgets; unpublished proprietary research
High Risk	Legally protected under FIPPA, or subject to regulatory or industry requirements such as PCI. Moderate harm if disclosed. Never share publicly. Select a sub-label.	Student IDs and grades; home addresses; identifiable face photographs; employee personal records; credit card transaction information
Very High Risk	Legally protected, or subject to regulatory or specific UBC security requirements. Significant harm if disclosed. Data steward approval required. Sharing must be auditable. Select a sub-label.	SIN; personal health information; biometrics; passwords; genetic data; bank details; government-issued identifiers

When content includes more than one type of information: choose the label that reflects the highest sensitivity in the content. If unsure, pause and consult UBC guidance or the accountable information owner or steward.

High Risk and Very High Risk: choosing a sub-label

Both levels require a sub-label. The sub-label records whether the information may leave UBC and under what conditions.



Sub-label	Handling	Examples
High Risk – Internal Only	For authorized UBC roles only. No external sharing.	Student grades; employee or student IDs; home addresses; face photographs; PCI card data; HR personal records
High Risk – External Sharing Allowed	Approved for external sharing under formal agreements.	Student or employee data with accreditors under contract; research data under a signed data-sharing agreement; PCI data with licensed processors
Very High Risk – Internal Only	UBC-only access. Data steward approval required. Sharing must be auditable.	SIN; personal health information; biometrics; bank details; internal passwords or keys; genetic data; government-issued ID numbers
Very High Risk – External Sharing Allowed	Trusted external partners only. Legal agreements and/or ethics approval generally required. Data steward approval required. Sharing must be auditable.	Health information under ethics-approved agreements; genetic or biometric research data under NDA and ethics approval; integration credentials exchanged with trusted partners

How to apply a sensitivity label to a file

Labels are applied directly in supported Microsoft 365 apps such as Word, Excel, and PowerPoint, and from Windows File Explorer for Office documents and PDFs.

- 1 Open the file**
in the Microsoft 365 app you normally use.
- 2 Find the Sensitivity control**
in the ribbon or sensitivity bar, and use UBC's label guidance.
- 3 Select the matching label**
If the file holds more than one type of information, choose the highest sensitivity present.
- 4 Review any prompt**
Policy tips, warnings, or handling instructions. Some labels add encryption, restricted access, or markings.
- 5 Save the file**
The label stays with the file across supported devices, apps, and cloud services.
- 6 Update if needed**
If the label later looks wrong, review the content and change it if you have permission.

Don't see the Sensitivity control? Labels may not yet be published to your account, the app or version may be unsupported, or the file type may not support labeling. Use the approved Microsoft 365 app and contact the appropriate UBC support channel if labels are expected but unavailable.



What labels do, and what they don't

What a label can do

A sensitivity label is more than a coloured tag. Depending on how UBC configures it, a label can support:

- Encryption and usage restrictions
- Content markings such as headers, footers, and watermarks
- Sharing controls and other compliance safeguards
- A consistent signal that future Data Loss Prevention policies can act on

You do not need the technical details to use labels well. Recognize the information, select the appropriate label, and follow the handling expectations that appear with it.

Labels are not a substitute for judgment

- A correct label does not make unnecessary access appropriate.
- A label does not fix every outdated permission or sharing link.
- Review the label when information changes, for example when confidential research is published.
- Over-labeling makes work harder and weakens confidence in the system.
- If a file is mislabeled, fix it or raise it with the owner rather than ignoring it.



Permissions, labels, and DLP work together

Permissions decide who can access a location or item. **Labels** describe how sensitive the information is and how it should be handled. Each control answers a different question.

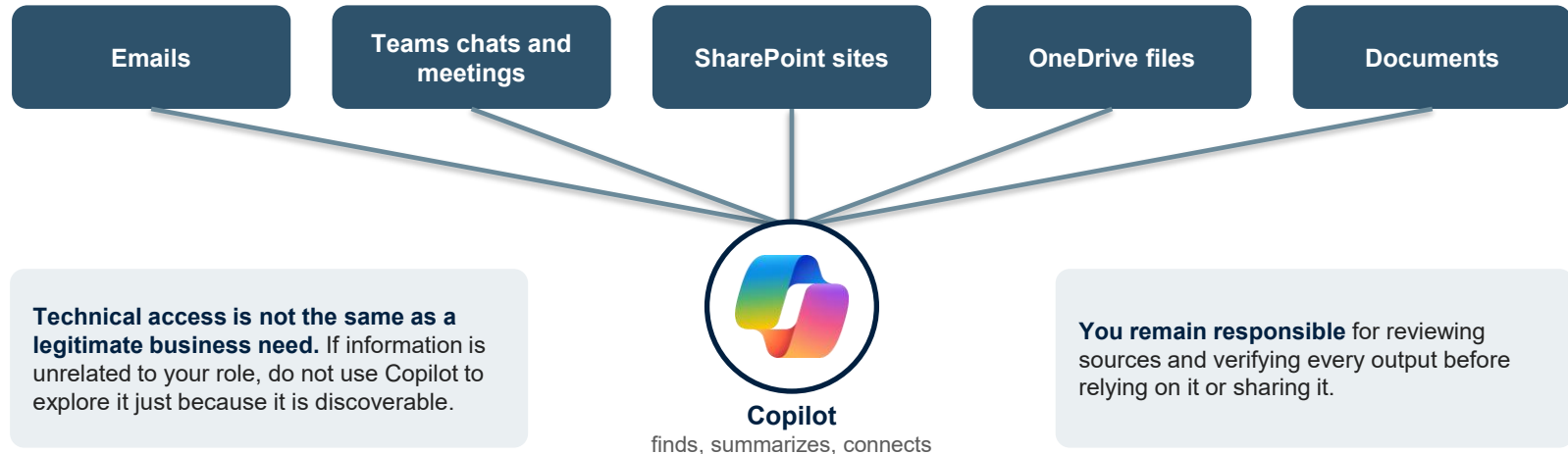
Control	Plain-language purpose	What it means for you
Permissions	Who can access the information	Share only with the people who need it and review access regularly.
Sensitivity labels	How sensitive the information is	Apply the label that matches the content and follow its handling instructions.
DLP safeguards	Helps prevent inappropriate use or sharing	Pay attention to warnings or blocks and do not try to work around them.
Records and lifecycle controls	How information is kept and managed over time	Store important information in approved locations and follow records requirements.
Responsible use	Why and how the information is used	Use information only for a legitimate UBC purpose and verify AI outputs.

DLP is not being switched on automatically. UBC's first priority is a shared classification practice: understand the information, apply the right label, and review who has access. That foundation enables future DLP policies and other automated safeguards. The goal is not to prevent legitimate work; it is to give information protection that matches its sensitivity wherever it is used.



Copilot works within the access you already have

Microsoft 365 Copilot helps staff and faculty work with information they already have access to in SharePoint, OneDrive, Teams, Exchange, and other Microsoft 365 products. It does not create a new permission system, but it can make permitted information easier to find and summarize.



Before you use Copilot: complete required training • use the approved UBC Copilot service and follow current guidelines • be clear about the purpose and information • confirm the source is appropriate • confirm who still needs access • verify the output afterwards

Why permissions still matter

Permissions decide who can open a file, folder, SharePoint site, Team, or other workspace. Copilot does not bypass them, but it may make permitted information easier to discover, so poor permissions carry greater consequences in an AI-enabled workplace.

Five common permission issues

People who have moved on

A site still includes people who no longer work on the project.

Shared too broadly

A folder is shared with a large group when a small team needs it.

Old links that still work

A sharing link outlives the purpose it was created for.

Copied to a less restricted place

A sensitive document loses the protection of its original location.

No clear owner

Nobody is accountable for reviewing membership and sharing.

A simple review checklist

- ☐ What information is stored here?
- ☐ Who owns or is accountable for it?
- ☐ Who currently has access?
- ☐ Does each person or group still need access?
- ☐ Are there external users or sharing links?
- ☐ Is the sensitivity label correct?
- ☐ Should anything be moved, archived, or deleted under records requirements?



Your responsibilities as a UBC employee

Technology supports responsible AI use, but it does not replace individual judgment. Each person remains responsible for the information used, the purpose of the task, and the quality of the result.



Do

- Understand the sensitivity of the information you work with.
- Use approved UBC systems and services.
- Apply sensitivity labels when required.
- Check permissions before using or sharing information.
- Use Copilot only for legitimate UBC business purposes.
- Verify AI-generated output before relying on it or sharing it.
- Ask your supervisor or the right subject-matter contact when the intended use is unclear.

Do not

- Assume an AI response is correct because it sounds confident.
- Use Copilot to make, recommend, or influence decisions affecting individuals, such as hiring, discipline, admissions, accommodations, or academic standing.
- Use Copilot to collect information about identifiable individuals from the web.
- Access information simply because Copilot makes it easy to find.
- Try to bypass a warning, restriction, label, or other safeguard.

Key takeaways

- Copilot works with information through the access you already have.
- Faster discovery makes good permissions and sharing practices more important.
- Sensitivity labels communicate how information should be handled.
- Permissions, labels, DLP, records controls, and responsible behaviour work together.
- Having access does not automatically create a legitimate business need.
- You remain responsible for reviewing sources, verifying outputs, and protecting information.

Remember

Classify the information.

Protect it according to its sensitivity.

Govern it throughout its lifecycle.

Use AI within those boundaries.



Your action plan

The most effective preparation for responsible AI is to review how your information is classified, who has access to it, and whether its label reflects its content.



Action	What to review	Done
1. Start with priority content	Identify files and workspaces containing student, employee, research, financial, legal, or other sensitive information.	☐
2. Review access	Check members, groups, external users, and sharing links. Remove access that is no longer needed.	☐
3. Confirm ownership	Make sure each important folder, Team, or SharePoint site has a current owner.	☐
4. Apply labels	Apply or correct the UBC sensitivity label that matches the highest sensitivity in the content.	☐
5. Improve storage	Move information to an approved, appropriately governed location when necessary.	☐
6. Make review routine	Repeat the review when projects change, people leave, information is published, or access needs change.	☐

Suggested first step: choose one SharePoint site, Team, OneDrive folder, or shared folder that you own or manage. Review who has access and whether key files carry the appropriate sensitivity labels.

Learn more

UBC AI Foundations, Module Five

The full training module, including five workplace scenarios and a knowledge check.

UBC Information Security Standard U1

The classification model behind UBC's sensitivity labels.

<https://cio.ubc.ca/information-security/policy-standards-resources/U1>

Microsoft Learn: Learn about sensitivity labels

<https://learn.microsoft.com/en-us/purview/sensitivity-labels>

Microsoft Learn: Microsoft 365 Copilot architecture and data protection

<https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-architecture-data-protection-auditing>

Microsoft Learn: DLP for Microsoft 365 Copilot and Copilot Chat

<https://learn.microsoft.com/en-us/purview/dlp-microsoft365-copilot-location-learn-about>

Questions about labels or Copilot at UBC? Contact your UBC IT Client Services Manager or the appropriate UBC support channel.





THE UNIVERSITY OF BRITISH COLUMBIA

Classify. Protect. Govern. Use AI within those boundaries.