



PIA Guidelines: Meeting Recording, Transcription and Assistant Tools

Overview

This document provides Privacy Impact Assessment (PIA) guidance for the expected use of meeting recording, transcription, and assistant tools at UBC. It helps ensure compliance with the BC *Freedom of Information and Protection of Privacy Act* (FIPPA) and UBC Information Security Standards, clarifying when a PIA is required.

Meeting assistant tools include software designed to support meeting activities through functions such as live transcription, summarization, task capture, and real-time captioning. Examples include Microsoft Teams Intelligent Recap and Zoom AI Companion, as well as third-party tools such as Otter.ai.

Key features of these tools typically include automatic speech recognition (ASR), live captioning, searchable transcripts, speaker labeling, and integration with productivity applications.

Authorized Tools

The following tools have been reviewed through the PIA process and are authorized for institutional use:

Purpose

Tool

Recording/Transcription

Microsoft Teams, Zoom

Meeting Assistant

Microsoft Teams Intelligent Recap, Zoom AI Companion

On-Demand Transcription

Microsoft 365 Transcribe in Word (Web Version)

When used under the following conditions, a PIA is not required:

- The tool is accessed through UBC's enterprise license (not through free-tier or personal accounts).
- Biometric features (e.g., speaker identification, voiceprint storage) are not enabled.
- The tool is not used to collect personal information from individuals outside the UBC community; Use is limited to faculty, staff and students.

Tips and Reminders

Only Record When Necessary

- Avoid recording meetings unless there is a clear operational or compliance need.
- Be especially cautious with sensitive topics (e.g., health information, grievances).
- Avoid recording personal conversations unrelated to University programs or activities.

Maintain Clear Identification and Privacy Notification

- UBC provides a general privacy notification to employees and students upon onboarding.
- A privacy notice is not required when using authorized tools in routine academic or administrative settings.
- If tools are used in non-routine-contexts or settings involving new populations (e.g., public-facing sessions, external stakeholders), consider whether a notification is appropriate based on the context and sensitivity.
 - **In practice, this can be done by including a short privacy statement in the meeting invitation or adding it to a participation consent form.**

Obtain Consent When Required

- Consent is not required to collect personal information necessary for UBC programs or activities.
- Informed consent is required to enable features involving biometric data (e.g. speaker identification, voiceprint analysis).
- For guidance on image use, review the Office of the University Counsel's [FAQ's: Consent to Use of Image Forms](#).

Align to [UBC Record Retention Schedules](#)

- Microsoft Teams and Zoom retain recordings for 12 months by default.
- Recordings should be treated as temporary aids to create official records (e.g. approved minutes, verified transcripts).
- Once an official record is created and saved to an authorized UBC system, the original recording must be deleted, unless longer retention is required by a UBC Retention Schedule.
- Chat messages are retained for 90 days before automatic deletion (per [Retention Schedule IM4700-30](#)).
- Recordings or chats must not be used as substitutes for official minutes or transcripts.

Grant Access to Data Sparingly

- Limit access to recordings and transcripts to individuals with a legitimate need-to-know.
- Do not share recordings externally unless explicitly authorized.

Accountability for Output

- Users of meeting assistant tools are responsible for reviewing summaries and transcripts **before** relying on them for decision-making or formal documentation.

Speaker Identification Requires Additional Safeguards

- Institutional tools must not enable biometric features (e.g., speaker labeling, voiceprint matching) unless a PIA has been completed.
- Consent must be obtained for tools offering speaker identification by name that have not been pre-authorized.
- A process must be in place to remove voice data when no longer needed (e.g., one-time guests, departing individuals).

Use for Immediate Transcription Only

- Tools not reviewed or authorized for institutional use may only be used for real-time transcription.
- Recordings or transcripts must not be stored or distributed through the tool's native platform.
- Transcripts must be promptly transferred to UBC-managed systems and deleted from the tool.
- Authorized tools (e.g., Microsoft Teams, Zoom) are subject to UBC-defined retention and security controls.

Avoid Use with Very High Risk Information

- Do not use meeting assistant tools to record or process Very High Risk information (as defined by [UBC ISS U1](#)) unless a PIA has been completed or additional safeguards are in place. (i.e., file encryption).
- Use should be limited to Low or Medium Risk information unless otherwise authorized.

(continued)

CAUTION: Use of Microsoft Word Transcription Feature

Ensure that the Optional Connected Experiences are disabled in the Office 365 account settings. This is especially important when handling sensitive information as Microsoft becomes the one deciding how the data is processed.

To disable, go to: *File* → *Account* → *Account Privacy* → *Manage Settings* → Uncheck ***Enable Optional Connected Experiences***.

Additional Resources

[Privacy Matters: Collaborate Securely Over Video](#)

[PIA Guidelines: Collaboration Tools](#)

[Records Management: Video Recording Best Practices](#)

MS Teams:

- [UBC IT Overview](#)
- [Learning Technology Hub Guide](#)
- [Records Management Best Practices](#)

Zoom:

- [UBC IT Overview](#)
- [Learning Technology Hub Instructor Guide](#)
- [Learning Technology Hub Student Guide](#)

Contact Us

For questions about this guidance, the PIA process, or to submit a PIA Inquiry, visit [Privacy Matters](#).