

Wisconsin Public Media Policy on AI Meeting Assistant Usage

1. Responsible use of the tool: AI meeting assistants may be used within Wisconsin Public Media when following these guidelines.

- The meeting host is responsible for informing all attendees that the tool will be utilized, and for ensuring appropriate use of the tool, including review, correction and validation, before any summarization document or other AI product is shared more widely, even with the rest of the meeting group.
- Meeting hosts should be aware of where the summarization product will be saved after the meeting, whether it will or will not be shared and be able to inform the meeting participants.
- Meeting hosts should never have the tool automatically distribute meeting summaries to all participants.
- Clients of Wisconsin Public Media cannot insist on using the tool.

2. Functionality & Approved Tools

AI meeting assistants are add-ons that use AI to make virtual meetings more efficient. In general, they do things like create post-meeting summaries and action item lists or answer questions about the meeting's content and context in the chat based on what the AI tools have "heard" at the meeting.

Wisconsin Public Media approves the use of the following tools, when utilized on UW-Madison's enterprise Zoom and Webex accounts:

- Zoom Meeting Assistant
- Webex Meeting Assistant

If you are interested in utilizing an additional tool, please consult WPM IT. All approved tools will be listed above, and any tool not listed above should be considered not currently approved for use.

3. Security and privacy

You may use approved AI meeting assistants, like those native to our enterprise Zoom and enterprise Webex, with HIPAA data, FERPA data and other internal, restricted and confidential data. Zoom and Webex meeting assistants have gone through a cybersecurity, compliance and legal review, as well as a review of existing business associate agreements.

Any use of an unapproved tool with internal, sensitive or restricted data poses serious data privacy risks. While university-approved tools have been reviewed to ensure that the vendor is accessing our data only at our direction, unapproved or consumer versions of a tool are likely sharing our information with the vendor for training their AI model and other purposes. Using an unapproved tool with internal, sensitive or restricted data can under some circumstances constitute a data breach.

4. Bias and error

AI Meeting Assistants and summarization tools are trained on models that contain bias and so the output of these tools can contain bias as well. These tools also make errors in their summarizations. Even if technically accurate, the tool can lack context to the extent that it does not provide a true picture of the tone and content of the meeting. Therefore, any record created by an AI tool must be reviewed, corrected and validated by a human before it is shared in any way.

5. Best practices

- Transparency and consent are part of the best practice etiquette around these tools. Meeting hosts should make sure that all participants are aware that an AI tool is being used at the meeting. If a participant objects to use of the tool, consider whether it can be turned off so that the meeting can progress.
- Some people are hesitant to be candid when a meeting assistant is present. Do not use the tool in situations where full and open discussion could be stifled.
- Be prudent with the tool.

6. Public records and records management

These AI tools are new and the Wisconsin public records law does not have specific statutes or cases that indicate how the summaries will be treated. The following represents UW–Madison’s current view. However, the Public Records Custodian always determines whether a document is a public record by using a fact-specific analysis on a case-by-case basis. For guidance related to specific use cases, contact the UW Records Officer, Public Records Custodian and the Office of Legal Affairs.

- The summaries created by the tool may or may not be public records depending on how they are shared and used. In general, the meeting host is responsible for the handling of these summaries and the meeting host’s use and distribution of these summaries will indicate whether they are not public records.
- If the summary is viewed by the meeting host only as a way to refresh their recollection of the meeting, the summary could be considered a personal note and would not be a public record. The meeting host may use the summary as a reference to create communications, including minutes as a follow-up to the meeting. The meeting host may delete the summary.
- If the meeting host decides to share the summary with others, assume it will be treated as a public record. It is the responsibility of the meeting host to review, correct and validate the summary prior to any sharing.
- The meeting host is responsible for ensuring that validated summaries shared with others, along with all other meeting materials, are managed throughout their lifecycle according to their appropriate records retention schedule.