

AI Meeting Recording & Notetaking Guidelines

Scope: These rules apply to all AI notetaking and meeting-transcription tools used across the group, regardless of platform (Zoom, Teams, Google Meet, Fireflies, or otherwise). The tool may change; these baseline rules do not.

Approved platforms

Zoom, Teams, Google Meet, and Fireflies are approved **only where you hold an Enterprise licence**. On an Enterprise licence, no additional licence or tool request is required. Free, personal, and consumer tiers are not approved, even for the same platform. Do not install or use any other AI notetaker for work meetings without approval, including free tools and any tool that auto-joins meetings from your calendar. If you want to trial something new, raise it first. Before use, confirm that the Enterprise account for the applicable tool includes a signed Data Processing Agreement (DPA) with your company and, for UK entities, ensure it configured to store and process data in the UK if this is available in the platform.

Data must not be transferred outside the UK or EEA unless appropriate safeguards (e.g. Standard Contractual Clauses) are in place. If you are unsure, check with Legal.

1. Notify everyone, and allow a genuine opt-out

Tell all participants that the meeting is being recorded and transcribed before it starts, and make clear that anyone can object and be excluded. Do not treat one person's say-so as permission for the room; each participant needs to be informed and able to decline.

Use a neutral, accurate automatic notification:

"This meeting is being recorded and transcribed by an AI notetaker so we can capture notes and actions. It may capture audio, video and a written transcript. If you'd prefer not to be recorded, please opt out or let the organizer know, and we'll stop. For further information, please see our Privacy Policy [insert link]"

Where possible, back this with a written notice in the calendar invite or a pre-meeting email:

"An AI notetaker will join this meeting to record and transcribe it for notes and actions. It may capture audio, video and a transcript, processed through [tool]. Data is retained for [30 days] and is not used to train AI models. You can object at any time by [clicking on this link/replying to this invite] or telling the organiser. For further information, please see our Privacy Policy [insert link]"

Take extra care with **external participants**: they never agreed to our tools, so flag the recording explicitly and stop if anyone objects. If your tool can send a pre-meeting consent email with an opt-out link, turn it on; it gives you an auditable record of notice and opt-out.

2. Permitted purposes

AI notetaking may be used for internal, external/client, and work or project-related meetings. It must **not** be used for:

- Interviews, performance reviews, or other HR matters
- Any meeting that may be privileged or sensitive, e.g. taking legal advice or discussing a dispute
- Any meeting likely to involve special-category data (health, trade union membership, and similar)

If you'd like to use it for any other purpose, or you're unsure whether a meeting falls into the above, check with Legal first.

3. Data minimisation and retention

Recordings and transcripts may capture personal data. Only record where there's a clear purpose, inform all participants beforehand, and delete transcripts and recording when they're no longer needed. Set data retention to 30 days as the default. If a meeting is a genuine project record you'll need beyond that, keep only what you need and note why.

Once you have checked the transcript and, if you wish, saved the notes or action points to your own files, delete the transcript, notes and recording from the platform, and in any event no later than 30 days.

4. High-risk data and DPIAs

Do not record meetings containing high-risk data (e.g. personnel data) without first doing a Data Protection Impact Assessment (DPIA). High-risk scenarios include, for example, processing special category data, and recording performance reviews or other HR meetings. Check with Legal if you are unsure whether you need one. See the AI Hub for guidance: <https://miroma-ai-hub.web.app>

5. Access and sharing

Restrict access to transcripts to those on a need to know basis. Do not share recordings or summaries beyond the relevant people who attended the meeting, relevant team or client group. Access should run through your work SSO account so that it's removed automatically when someone leaves.

6. Client material

If a transcript contains client material, check the client contract for any restrictions before using or distributing it. Some contracts restrict where data can be stored or processed, which affects which tool you can use.

7. Human sign-off

AI notetakers make mistakes, especially with names, numbers, and who said what. Always review AI-generated summaries before acting on them or sharing them. A summary is not an authoritative or verbatim record.

8. Use your work account only

Do not enable transcription features on personal Microsoft, Google, or other accounts.

9. Raising concerns

Any concerns about how transcript data is stored or shared should go to your IT provider. If personal data is involved, copy Legal.

Where a data breach or suspected non-compliance is identified, escalate immediately to Legal and your IT provider so that any notification obligations to the regulator can be assessed and met within the applicable statutory timeframes.

10. Review

These guidelines will be reviewed periodically and updated to reflect changes in technology, legal requirements, or organisational practice.