AI Note-Taking in the Workplace

AI meeting assistants can turn spoken discussions into summaries and action lists. They can also capture sensitive employee, customer and commercial information. Employers need clear rules about when recording or transcription is appropriate, who can access the result and how errors are corrected.

1. Agree the purpose before switching on an assistant

Explain whether the tool will record audio, produce a transcript, generate a summary or extract tasks. Make sure the purpose is necessary, proportionate and covered by an appropriate lawful basis under UK data protection law. A product being available inside a meeting application does not, by itself, authorise its use.

Question before use	Practical employer control
Who is participating?	Tell participants clearly what is being captured and why.
What information might be discussed?	Assess personal, sensitive employment and commercially confidential material.
Where will records be stored?	Check suppliers, access permissions, international transfers and retention settings.
Can the output be challenged?	Make a named person responsible for checking and correcting important conclusions.

2. Do not treat an AI summary as an agreed record

Automatic transcription can misidentify speakers, omit qualifications and convert suggestions into apparent commitments. Where a meeting may affect an employee, verify critical statements against notes, relevant documents and the participants' responses. Give the people concerned a fair opportunity to correct material inaccuracies.

Example A | A return-to-work conversation

An AI summary states that an employee agreed to resume full duties immediately, but the discussion actually included a phased-return proposal.

Employer response: The manager checks the transcript and written follow-up, confirms the agreed hours with the employee and corrects the HR record before relying on it.

3. Keep workplace and HR data protected

Set clear permissions and retention periods; restrict any highly sensitive recording or transcript to those with a genuine need. Follow your privacy notice and complete a data protection impact assessment where the processing is likely to create a high risk. A confidential grievance or medical meeting requires particular caution.

- Do not upload confidential employee records into an unapproved personal AI account.
- Avoid recording private or sensitive meetings by default; assess the need first.
- Do not use an unchecked AI summary as the sole evidence for a disciplinary decision.

4. Adopt a short, workable meeting policy

Your policy should specify approved tools, permitted meetings, the information given to participants, how objections or concerns are managed, review and correction responsibilities, retention, deletion and access permissions. Train managers and audit how the controls work in practice.

Discuss your workforce requirements with Assyst

Assyst Workforce Management is a workforce management platform for multi-site employers, bringing together HR and paperless onboarding, time and attendance, workforce scheduling, payroll calculations, task management and a mobile staff app. To find out more or discuss how Assyst could support your business, visit www.assyst.uk and contact us through the website.

Useful official sources

ICO — Data protection and monitoring workers
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

ICO — Collecting and keeping employment records
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/employment-practices-and-data-protection-keeping-employment-records/collecting-and-keeping-employment-records

ICO — UK GDPR guidance and resources
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

General guidance for employers in Great Britain, reviewed November 2026. Contract terms and individual circumstances may require professional advice.