CHSCP Minimum Standards Policy:
Use of AI for Meeting Recording and Transcription

1. Introduction and Purpose

This policy establishes the **minimum standards** for the responsible, secure, and ethical use of Artificial Intelligence (AI) tools to record, transcribe, and summarise meetings within the City & Hackney Safeguarding Children Partnership (CHSCP).

Recognising that SCP meetings involve some multi-agency partners using different technical ecosystems, (primarily **Microsoft Teams**, **Google Meet**, and **Zoom**), this document ensures a consistent approach to data protection, regardless of the platform used.

This policy acknowledges that individual Partner organisations maintain their own internal policies regarding the utilisation of AI. The guidance contained in this policy is not designed to supersede or override existing agency specific AI policies. It serves to assure all Partners that the CHSCP administrative staff will operate strictly within established data protection parameters, thereby mitigating risks associated with AI usage in a multi-agency context. Partners should primarily adhere to their own organisational policies, using this policy guidance for assurance purposes.

1.1 Scope

This policy applies to:

- **Strategic Meetings:** Board meetings, sub-groups, and partnership business meetings.
- **Operational Meetings:** Multi-agency case audits, strategy discussions, and complex case reviews where personal data regarding children and families is discussed. However, participants must adhere to established professional practice for data minimisation, including the use of initials for children, and generic descriptors such as 'mother,' 'father,' or 'sibling' for family members.

Note: Specific high-sensitivity contexts (e.g., ongoing criminal investigations or legal planning meetings) may require a total prohibition of AI recording. Refer to Section 4 for exclusions.

2. Core Security Standard: The "Closed Environment"

The CHSCP requires a ‘Closed AI Environment’ for all meeting transcriptions. Public-facing, "open" AI tools that use user data for model training are strictly prohibited for safeguarding business.

2.1 Approved Platform Architecture

Any AI tool used for CHSCP business must meet the following technical criteria:

- **Enterprise Instance:** The AI must operate within a managed, enterprise-level tenancy (e.g., Microsoft Copilot, Gemini for Google Workspace, or Zoom AI Companion Enterprise).
- **No Model Training:** The provider must legally guarantee that audio, transcripts, and prompts are **NOT** used to train their public Large Language Models (LLMs).
- **Data Sovereignty:** Data processing and storage must adhere to UK GDPR requirements (e.g., stored within the UK or adhering to the EU Data Boundary).

- **Governance and Due Diligence:** Prior to enabling or using any AI recording/transcription/summarisation capability for SCP meetings, the Host Organisation must complete documented due diligence and obtain formal approval through its local information governance and digital assurance route. Evidence of approval must be retained for audit and reviewed when the platform, AI feature, supplier terms, or data processing arrangements change (or at least annually).

2.2 Unauthorised "Bot" Prohibition

The use of unauthorised third-party AI ‘scribes’ or ‘bots’ (e.g., Otter.ai, Read.ai, Fireflies) that join meetings as external participants are **strictly prohibited**. Meeting hosts must remove any unauthorised AI participants immediately upon detection.

3. Data Protection and Sensitivity Classification

Given the multi-agency nature of the partnership, the following standards apply to data handling:

3.1 Data Controller & Processor

- **The Host Organisation** acts as the Data Controller for the recording and transcript.
- **The Platform Provider** (Microsoft, Google, Zoom) acts as the Data Processor.
- Partners attending the meeting agree to the Host Organisation’s data governance policies for that specific session.

3.2 Review and Validation Standard

AI transcripts are never the definitive legal record until validated.

- **Human Moderation:** All AI-generated summaries must be reviewed by a human professional (e.g., the Chair or designated minute-taker) for accuracy and context.
- **Disclaimer:** Unverified drafts must carry a clear watermark or header: *"DRAFT: AI-Generated - Subject to Human Verification."*

3.3 Access Controls

Access to recordings and transcripts must be restricted based on the *Need-to-Know* principle.

- Links to recordings must **not** be open to ‘Anyone with the link.’
- Access must be limited to invited attendees and designated administrative support staff.

- Online meetings organised by administrative staff, will be configured to guarantee that only the meeting organiser or ‘host’ will receive meeting artifacts (including transcription, audio video recording, and AI note taking products). This option is available in both Google Meets and MS Teams.

- A new standing item shall be incorporated into all meeting agendas to ensure the Chair and administrative support are prompted to terminate the meeting recording once formal business has concluded, thereby safeguarding the privacy of any subsequent post-meeting discussions

4. Notification and Consent

Transparency is mandatory to maintain trust between professionals and with families (if present).

4.1 Advance Notice

Meeting invitations must state if AI recording tools will be utilised.

Standard Wording: "This meeting may be recorded and transcribed using [Platform Name] AI assistance to facilitate accurate minute-taking. Data is processed within a secure, closed enterprise environment."

4.2 The ‘Start of Meeting’ Protocol

The Chair/Host must perform the following checks before activating AI tools:

- Announce that the meeting will be transcribed for administrative purposes.
- Explicitly ask if any partner objects.
  - *Police/Legal Veto:* If a police partner or legal representative objects due to the discussion of live criminal proceedings or legal privilege, the recording **must not** proceed.
- Advise participants that voice attribution is active.

4.3 Handling Objections

If a participant objects to the recording:

- The recording must be stopped or paused immediately.
- The Chair must facilitate a consensus (e.g., manual note-taking for the sensitive section, or the whole meeting).

5. Retention and Deletion Standards

To comply with the UK Data Protection Act 2018 and minimise risk, the CHSCP enforces strict storage limitations.

a) Original Audio and Video Recordings These materials are strictly temporary. The Meeting Host or Chair is responsible for managing these files. The maximum retention period is 30 days; however, the primary rule is that all audio and video recordings should be deleted immediately after the written minutes have been ratified.
b) Transcripts generated by AI are considered working documents intended solely for verifying the accuracy of the minutes. The Minute Taker or Admin Support holds the responsibility for these files. They must be deleted as soon as the official record is agreed upon, with a strict maximum retention limit of 90 days.
c) To provide assurance that records have been destroyed, participants will have access to a record of deletion notices. These will be held in a shared folder maintained by administrative staff. See here.

d) Unlike the temporary recordings and transcripts, the final minutes represent the permanent record. The Host Organisation is responsible for retaining these documents in accordance with their specific retention schedules. This varies by context; for example, standard corporate retention applies to general business meetings, whereas sensitive files, such as those regarding Child Protection, may be retained for up to 75 years.

5.1 Legal Holds

In the event of a Serious Case Review, Child Safeguarding Practice Review, or criminal investigation, a 'Legal Hold' may be placed on all data. In such cases, the automatic deletion of audio/transcripts must be suspended until advised by the Legal Team.

6. Acceptable Use Summary

To ensure clarity for all professionals, the following 'Traffic Light' system applies:

GREEN (Permitted):

- Routine business meetings.
- Partnership Board meetings.
- Training sessions.

AMBER (Caution - Chair Approval Required):

- Strategy discussions involving family details.
- Multi-agency audits.
- ***Requirement:*** Ensure all attendees are verified professionals.

RED (Prohibited):

- Meetings involving Covert Human Intelligence Sources (CHIS).

- Discussions regarding active, high-risk police operations where evidential chains are paramount.
- Whistleblowing interviews requiring guaranteed anonymity.

Document Version: 1.0
Date of Issue: February 2026
Status: Active
Applicable To: All Partner Organisations (Local Authority, Health, Police, Probation, Education, Voluntary Sector) and participating staff.