Cumbria Fire & Rescue Service

Information Security Month October 2025

Newsletter 5 | Who's in your Meeting?

Welcome to the fifth and final newsletter to be shared with you during October to mark Information Security Month.

Information Security Month is an international initiative aimed at raising awareness about cyber security threats and educating individuals and organisations on how to protect themselves.

The theme of this final newsletter is Information Security – Who's in your Meeting?

In this newsletter you'll learn about:

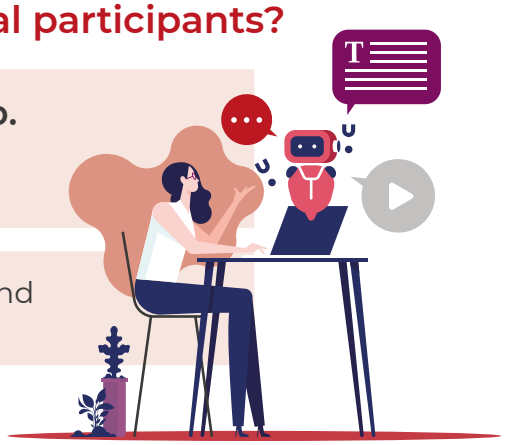
- Being wary of AI bots which may join a Teams meeting with external participants such as Otter AI and Read AI bots
- What to do if you find yourself in this situation
- Teams meeting etiquette – recording and transcribing meetings
- Consider whether you want to use a lobby or prevent auto-forwarding of the meeting invite
- Good practice reminders.

What is a record?

Attending a Teams meeting with external participants?

Check who (or what!) has turned up.
We are seeing an increase in AI bots joining meetings alongside external participants.

Ensure unauthorised AI bots such as Otter and Read.ai are dismissed from the meeting.

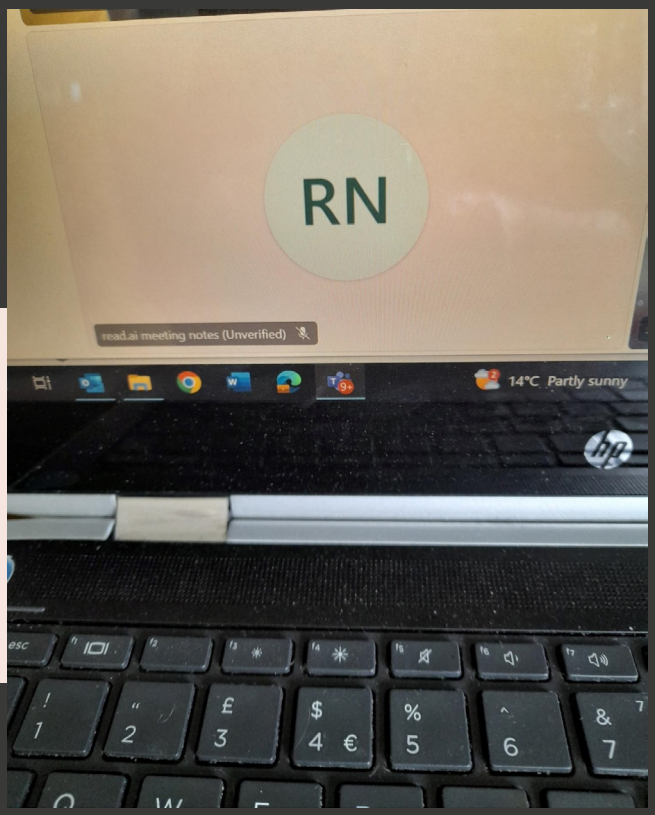


Making Cumbria a safer place for all

cumbriafire.gov.uk

CASE STUDY 1

This AI bot appeared in a Teams meeting set up by a staff member. Internal and external participants were invited to the meeting. The AI bot joined the meeting alongside an external participant who hadn't even realised that they had signed up to having an AI bot.



The bot looks like an ordinary user (initials in a circle).

The small text at the bottom gives it away:
"read.ai meeting notes (Unverified)"

Note that some bots may be harder to spot if they have an ordinary name!

In this case, staff realised that the AI bot was not a human participant and expelled it from the Teams meeting. This was a near miss. If the AI bot had not been expelled, sensitive information discussed in the meeting could have ended up anywhere in the world.

Information from the meeting would have been shared with all the external and internal participants as minutes, potentially including names and images of the participants, matters discussed, tasks, outcomes etc. Where the AI service is storing the information and where participants are storing the information may not be secure.

Information recorded by the AI bot could potentially be used to train AI models. An AI model is a computer program which is fed large amounts of data so that it can "learn" and make decisions / generate content / make predictions / give advice etc.

If the AI bot had not been expelled and sensitive / personal / confidential information was discussed, this would have amounted to a data breach. Consequences of a data breach can include damage to our reputation, large fines, and sensitive information being released publicly.

If an external participant uses an AI bot such as Otter or Read, the AI bot may be able to join the meeting even if the external participant declines the meeting and does not attend (the AI bot can potentially join in the participant's place).

It is very important to check the identity of all participants who join a meeting including external participants, particularly if the meeting includes sensitive content. This can be very difficult if it is a meeting with a large number of participants. Please see meeting etiquette below for tips such as having a lobby, checking names of participants, perhaps asking participants if they will turn on their camera or speak to verify themselves.

CASE STUDY 2

Otter AI taken to Court in the USA

In a recent lawsuit in the USA, Otter AI was accused of using its "Otter Notetaker" and "OtterPilot" AI transcription tools to record and transcribe meetings without obtaining consent from all participants.

The complainant alleged that non-account holders were captured on recordings, and that these recordings were then used to train the company's AI models, raising significant questions about data use and privacy compliance.

For organisations using AI notetaking tools, the key take-aways are clear: you must ensure any use of such tools is covered by appropriate consent from all meeting attendees, understand how the vendor uses and stores the data (especially if reused for AI training), and review whether your policies cover these scenarios.

Cumbria Fire & Rescue Service does *NOT* approve users to have these external tools to record Teams meetings. Meetings can be recorded, transcribed and summarised within Teams by selecting "Record and transcribe" and "Start recording" once the meeting has started with prior approval from participants.

We still need to be wary that external participants (individuals and companies) who use such tools may bring them along to meetings. If sensitive/personal/ confidential information is to be discussed, these AI bots should be dismissed / the meeting terminated, and ICT / Information Security should be contacted for advice.

AI Notetaking Tools Under Fire: Lessons from the Otter.ai Class Action Complaint | Workplace Privacy, Data Management & Security Report

Meeting etiquette

Recording Meetings and AI Use

Why this guidance matters

Meetings often involve the discussion of sensitive information – about our colleagues, residents, partners or the service. With the increasing use of recording features, AI transcription tools, and external bots, we need to ensure we protect privacy, maintain trust, stay compliant with data protection legislation and protect sensitive/confidential information from being leaked.

This guidance sets out the **etiquette and rules** for recording meetings, handling transcripts, and the use of AI in meetings.

Internal Meetings

1/ Recording and Transcribing

Always declare upfront: If a meeting is to be recorded (audio, video, or transcript), the organiser **must clearly state this at the start** of the meeting and/or in the meeting invite. Notification must be given **before** the recording commences.

Consent is required: Participants must be given the option to opt out or request that recording is stopped. If external participants do not consent, the recording cannot go ahead.

Purpose must be clear: Explain why the recording is being made (e.g. "for accurate minutes" or "to support accessibility") and state who will be given access to it.

Duration of retention: Explain how long the recording will be kept.

Only use Authorised Tools: Internal meetings can be recorded, transcribed and summarised within Teams by selecting "Record and transcribe" and "Start recording" once the meeting has started with prior approval from participants.

2/ Use of AI Tools in Meetings

For security reasons, **AI transcription or note-taking services that are not managed by our ICT department must not be used in internal meetings without prior authorisation from ICT / Digital / Information Security.**

Internal AI transcription tools (such as Microsoft Teams' built-in transcription) can be used, but:

- Participants must be notified at the start
- Transcripts should be used only for the agreed business purpose
- Do not copy or upload transcripts into non approved AI tools.

3/ Outputs - Transcripts, Notes, and Summaries

Retention

Meeting transcripts and summaries should be retained only as long as needed for their intended purpose.

Storage

They must be stored in secure, approved locations (e.g. SharePoint, Teams channels, or approved document repositories). Do not store on personal drives or unapproved apps. Where recordings are automatically saved to individual users' OneDrive accounts, these should be either moved to more suitable storage (e.g. SharePoint) or removed within a suitable timeframe.

Sharing

Only share meeting outputs with participants or those with a clear business need. Where a meeting recording (or any transcript/notes of a meeting) is to be shared with people/teams not included in the original call, this should be communicated to the attendees at the start of the recording.

AI Use

If AI is used to generate summaries or notes, this must be done within approved platforms that are governed by our ICT and data security standards (e.g. Copilot Chat in your Edge browser – check for the green shield which confirms that information entered is secured).

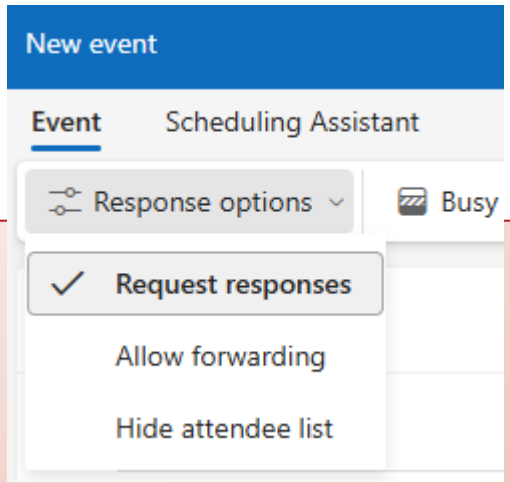
4/ External Meetings

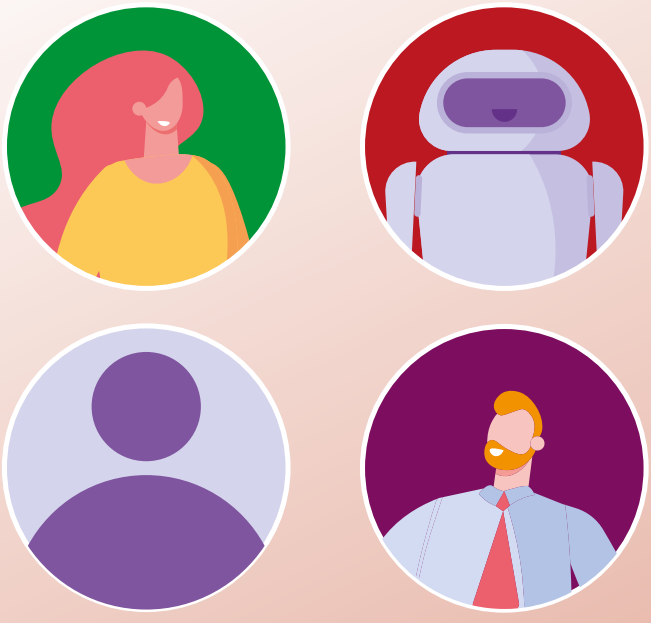
Recording or transcription must **not** proceed without explicit agreement from all external participants. **Unauthorised external AI bots such as Otter and Read.ai are not permitted.** If an external participant brings an AI bot to the meeting, ask for it to be removed or disabled if possible. If it cannot be disabled and the meeting contains sensitive/personal/confidential information, the meeting should not proceed. Please ask ICT / Information Security for guidance.

Consider the lobby – if you set up a meeting with external participants, as meeting organiser you can set up a lobby so that external participants do not automatically join the meeting. You review who they are and let them into the meeting if you are expecting them. If you are unsure about any of the participants, query it. Could one of them be an AI bot disguised with a human name?

Ask participants to verify themselves – review the participant list and if you are unsure about the identity of external participants, ask them to confirm their identity e.g. by turning on their camera or by speaking. Ask external participants to confirm whether they are using their own AI bot / transcription tool such as Otter or Read. This is important if the meeting will contain sensitive / confidential information.

Consider whether to allow forwarding – Do you want external participants to be able to forward our meeting request on to others?





5/ Good Practice Reminders

Be transparent: Always declare recording or transcription at the start.

Be proportionate: Only record if there is a genuine business or accessibility reason.

Be protective: Treat transcripts and notes as sensitive records.

Be compliant: Follow our AI and data governance policies at all times.

Be mindful: Do you recognise all participants?

In summary:

- No silent recording or transcription
- No unauthorised external AI bots/ services
- All transcripts and summaries are treated as sensitive information
- Use only approved systems (Teams, CoPilot, SharePoint, etc.).

By following this guidance, we can ensure our meetings remain safe, transparent, and compliant - protecting both our organisation and the people we serve.

Information Security Month 2025

#StrongPasswords #CyberAware #BrowseSafe #ThinkCyber
#MindfulClicks #OwnYourSecurity