Committee	Audit & Risk Management Committee		
Date paper prepared	04/08/2025	**Date of committee meeting**	20/08/2023
Subject	Incident report and actions taken following Read.AI bot incursion		
Author	ICT Services Manager, Kate Hannay.		
Action requested	I. Report on incident, actions taken, remediation, and future prevention.		
Purpose of the paper	To advise committee members and board of results of investigation and actions taken following third-party external incursion of an AI bot into A&RM meeting 27/5/25		
Summary of the paper	Timeline of incident event. Immediate actions taken. Preventative actions applied. Discussion on further recommendations.		
Consultation	UHI North, West and Hebrides ICT Manager Kate Hannay and Principal Lydia Rohmer, in consultation with: UHI Executive Office: Director of IT and Digital Infrastructure John Maher Head of IT Services and information Security Jem Taylor Unified Communications Engineer Leanne MacLeod and Technology Enhancement and Delivery Manager Roray Stewart		
Resource implications	Nonspecific resource requirements, though repeated messaging and comms to remind staff of best practice when organising meetings recommended.		
Risk implications	Failure to enforce policy and procedure recommendations could lead to further unauthorised participation in sensitive meetings conducted via Teams, resulting in potential data or identity theft, and risking leak of confidential information to external individuals or organisations possible ransom, media leaks or wider inappropriate dissemination.		

Link with strategy	
Equality, Diversity, and Inclusion	Ensuring our documents can be read and understood by everyone, including people with disabilities or impairments, is a legal requirement under the Equality Act 2010.
Island Community Impact	Not required in this instance. See the Island communities impact assessments: guidance and toolkit - gov.scot (www.gov.scot)
Paper status	☒ **Open – The paper may be circulated to non-members of the committee and published online without restriction.** ☐ **Restricted** – The paper must not be circulated to non-members or published online until after the committee meeting. ☐ **Confidential** - The paper must not be circulated beyond the committee members and should not be published online. Some information is considered commercially sensitive. [Please note papers may still be subject to Freedom of Information requests – see below].
Freedom of information	Choose an item. FOISA exemptions | Scottish Information Commissioner (itspublicknowledge.info) If closed/ withheld, select date this will become 'open': Enter a date.

Read.AI bot incident May 27th 2025

Terminology and nomenclature:

Bot – short for "Robot", in this case a reference to an automated function run as part of an application.

AI – Artificial intelligence, a catch-all term to describe automated functions or services utilising Large-Language Models (LLM) to perform a task.

Teams-Addon – a bolt-on third-party software application applied to a Microsoft Teams client to add additional functions or tools.

LR – NWH Principal

KH – NWH ICT Services Manager

EC – NWH Board Secretary

ITDI – IT and Digital Infrastructure group

Summary of Incident:

On 27/5/25 during a scheduled Audit & Risk Management committee meeting, in which confidential and sensitive information is presented in a Microsoft Teams conference call, an unknown entity joined the call. This entity was identified as **read.ai meeting notes (Unverified).** When no further identification or ownership was determined, the entity was removed from the meeting and did not return. Concerns were raised with UHI NWH ICT Manager, and an investigation instigated in collaboration with colleagues at UHI ITDI.

Read.AI is a genuine application deployed as a Teams-Addon. It facilitates the recording of meetings, monitoring chat/messages, attachments, and emails, utilising these to construct an "AI" Summary of the meeting. This summary would be complete with identifiable participant information and content. It is generally used as a tool to enhance the creation of meeting minutes.

The initial concerns were centred around privacy; participants noted that ownership of the bot was not clear and use of the bot to record minutes was neither approved nor would have been appropriate in this committee meeting. The follow up investigation of the incident raised additional concerns as outlined in this report.

Meeting and Participant Information:

Meeting title	Audit & Risk Management Committee Meeting
Attended participants	12
Start time	5/27/25, 4:59:37 PM
End time	5/27/25, 7:37:17 PM
Meeting duration	2h 37m 40s
Average attendance time	1h 30m 50s

Name	First Join	Last Leave	In-Meeting Duration	Email	Participant ID (UPN)	Role
Ellen Campbell	5/27/25, 4:59:40 PM	5/27/25, 7:24:53 PM	2h 17m 59s	Ellen.Maclean@uhi.ac.uk	NWH12EM@uhi.ac.uk	Presenter
Neil Hope	5/27/25, 5:00:22 PM	5/27/25, 7:37:16 PM	2h 36m 53s	NEIL.HOPE@uhi.ac.uk	EX01NH@uhi.ac.uk	Presenter
Ian MacEachern	5/27/25, 5:00:54 PM	5/27/25, 7:17:26 PM	2h 12m 51s	EX06IM@uhi.ac.uk	EX06IM@uhi.ac.uk	Presenter
Kevin Mallett	5/27/25, 5:09:22 PM	5/27/25, 7:17:26 PM	2h 8m 4s	Kevin.Mallett@uhi.ac.uk	NWH18KM@uhi.ac.uk	Presenter
read.ai meeting notes (Unverified)	5/27/25, 5:13:34 PM	5/27/25, 5:16:29 PM	2m 54s			Presenter
Lydia Rohmer	5/27/25, 5:14:16 PM	5/27/25, 7:37:17 PM	2h 23m 1s	LYDIA.ROHMER@uhi.ac.uk	NWH4LR@uhi.ac.uk	Presenter
Scott McCready	5/27/25, 5:15:10 PM	5/27/25, 6:08:30 PM	53m 19s	smc@wbg.co.uk	smc@wbg.co.uk	Presenter
Rotherham, Tom	5/27/25, 5:15:28 PM	5/27/25, 5:41:11 PM	25m 43s	twrotherham@deloitte.co.uk	twrotherham@deloitte.co.uk	Presenter
Derek Bond	5/27/25, 5:16:04 PM	5/27/25, 7:17:27 PM	2h 1m 23s	DEREK.BOND@uhi.ac.uk	NWH4DB@uhi.ac.uk	Presenter
Sarah Fraser	5/27/25, 5:41:21 PM	5/27/25, 7:17:46 PM	1h 30m 24s	Sarah.Fraser@uhi.ac.uk	EX12SF@uhi.ac.uk	Presenter
Tracy Kerr	5/27/25, 5:41:25 PM	5/27/25, 6:30:10 PM	48m 45s	TRACY.KERR@uhi.ac.uk	NWH1TK@uhi.ac.uk	Presenter
Jim Hutton	5/27/25, 5:41:26 PM	5/27/25, 6:30:10 PM	48m 44s	Jim.Hutton@uhi.ac.uk	NWH1JH@uhi.ac.uk	Presenter

The Teams meeting was initiated at 1649 by Board Secretary Ellen Campbell, started in advance of the scheduled start time for preparation. Committee members continued to join between 1700-1741. This included two known external (non-UHI) participants who were invited to this specific meeting.

Summary of Investigation

27/5/25

- At 17:13 “read.ai meeting notes (Unverified)” joined the call.
- Board secretary queried participants on knowledge of the entity, all replied unfamiliarity of it.
- At 17:16 after 2 minutes 54 seconds connection to the meeting Board Secretary ejected the entity from the meeting when it was confirmed no member present had knowingly utilised it for the call.
- The meeting continued as normal until 19:37.
- Board secretary in agreement with Principal emailed NWH ICT Manager that same evening of 27/5/25 at 20:05.

28/5/25

- ICT Manager instigated investigation the morning of 28/5/25, providing initial response to Principal and Board Secretary by 10:14.

29/5/25

- Investigations completed, recommendations issued to Board Secretary and Principal, further observations to continue at partnership level.

Investigation process:

- KH contacted UHI Unified Communications team to review logs, and begin investigation into how bot gained entry, whom it was associated with, and any preventative measures.
- KH raised concerns with UHI Director of IT and Digital Infrastructure John Maher and UHI Head of IT Services and information Security Jem Taylor.
- KH and EC engaged in conversation with UHI Unified Comms Team to retrieve additional information, resulting in KH arranging confidential access to NWH Board Teams/Outlook account to retrieve evidence.
- UHI Unified Comms raised ticket with Microsoft Premier Support to attempt to determine ownership of the Read.AI account utilised.

Investigation Findings:

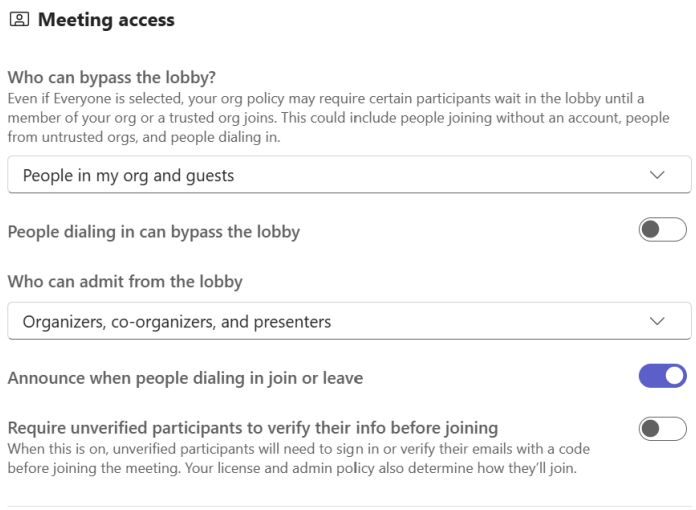
UHI blocks non-approved Teams-addons by default within its tenancy and userbase, so no UHI account holder can install non-approved addons without specific approval and actions taken by the ICT team.

A user utilising their own personal account, or via an external organisation’s tenancy account could potentially utilise addons that would not be within UHI or local ICT control to block.

Of the participants in the meeting on 27/5/25, all but two were UHI account holders. These two accounts were invited guests to the meeting, and stated on the call and afterwards that they had no knowledge of the Read.AI application or used it.

It was uncovered during this investigation that when an external participant using Read.AI is invited, their Read.AI is able to also join the meeting as a guest. This remains the case even when the invited participant does not attend the meeting themselves. This function presents significant risk to UHI NWH with potential to breach GDPR rules, Data Protection, and privacy or confidentiality expectations. Even when these issues are not breached, recording of the meeting in this manner fails to request or receive permission from other meeting participants.

The mechanism through which the bot was able to join the call was due to the defined permissions of the meeting. In any Teams meeting several 'Meeting Access' options are available to the organiser. The screenshot below indicates the default settings.



The crucial element here is the "Who can bypass the lobby?" option. **In the A&RM meeting in question, this option was set to "Everyone".** By default, the setting is "People in my org and guests". This setting means that individuals within the same tenancy (UHI) are able to freely join the meeting without actively being admitted by the meeting organiser or any present participants. An individual who has received the invite (either by direct invitation or forwarded to them) may join the meeting without any form of further permission. This default setting is the standard practice across UHI and industry in general.

The full set of available options are:

Everyone	Any individual with a link to the meeting/invite.
People in my org, Trusted orgs, and guests.	Any individual in the organisation tenancy (UHI), another organisation with approved trust (e.g. NHS, HIE), and/or external guest who has received the invitation link.
People in my org and guests	Any individual in the organisation tenancy (UHI), and/or external guest who has received the invitation link.
People in my org.	Any individual in the organisation tenancy (UHI) who has received the invitation link.
People who were invited.	Only individuals specifically invited. Forwarded invites by invitees are not permitted.
Organisers, co-organisers, and presenters.	Only the meeting organiser, delegated co-organisers, or nominated presenters that have received the invitation link.

Due to the selected setting for the meeting on 27/5/25 being set to “Everyone”, any individual that had access to the invite email would be able to join the meeting without restriction or moderation. The choice to enable this setting was based on a misapprehension by the meeting organiser regarding external access to the meeting. This setting allowed the external participants to join without being held in a lobby pending approval to admit from internal meeting attendees.

This permission setting also allowed the Read.AI bot to join the meeting without it needing to request permission to join.

At this stage, the investigation had discovered the mechanism through which the bot was able to join the meeting, but further investigation was required as to where this specific instance of the Read.AI bot originated.

Further Information to the Investigation

1. From investigations conducted by UHI Unified Comms, the Read.AI bot is supposed to identify itself in the Teams chat upon connection, state its purpose, and the account it is associated with. Participants note that the bot that joined the meeting on 27/5/25 did not do these actions.
2. The Read.AI bot had no associated email account in its designation.
3. Participants in the meeting stated no association with the bot.
4. For the 2 minutes 54 seconds the bot was present in the call it should be assumed that it recorded the names of the other participants, recorded any conversation that occured, transcribed that information, and produced a summary for its “owner” of that conversation before it was removed from the meeting.
5. The “Owner” in this instance remains unknown.

Plausible reasons for the bot joining the meeting

The following represent the likely origins of the ReadAI bot:

1. Possibility an external participant did not know they were using the Read.AI bot addon. This is unlikely, and there was no link in the bot’s designation to match any of the participants.
2. Possibility of an intentional malicious attempt to gain access to a sensitive meeting for the purposes of fact-finding. This could be instigated by someone utilising the bot for this purpose or alternatively creating a Teams account named to match the Read.AI bot designation in the hope of fooling meeting participants into accepting the presence of the bot.
3. A random attack, operated remotely, that has not specifically targeted this meeting or UHI NWH. In this scenario, a bot may be set to attempt to attend any random “open” meetings running on Microsoft service. This is considered the least likely of the possible origins.

Risks associated with the event

1. If the bots use was intentional or unintentional without malice, there remains a GDPR and Data Protection concern about the use of an external party utilising the tool to record the meeting without the consent of the participants. This is a policy rigorously enforced within UHI.
2. We cannot ascertain the source/owner of the bot or account associated with it, so remain without indication of the intent or origin. Microsoft would not disclose any details relating to the account for reasons of user privacy.
3. For the 2 minutes 54 seconds duration of the bot being connecting to the meeting, any conversation during that point has possibly been recorded by this entity. From discussions with EC following the event the meeting was in pre-start phase with not all participants yet in the call, so content was informal non-business related mostly centred around the discovery and attempts to identify the bot. It is considered unlikely that confidential information was disclosed in this instance.
4. We are faced with the concern that the most plausible origins indicate that either the invite was intentionally shared with a third-party who utilised the bot or impersonated the bot to join the meeting, or that the invite was leaked through other means.

Actions taken and lessons learned

1. KH confirmed with UHI Unified Comms default block on non-approved Teams addons was in place, verifying that it could not have been a UHI account holder responsible for the bot.
2. KH discussed and agreed with UHI Unified Comms and ITDI that default position for Teams calls where external participants are involved should be No lobby bypass for external connections.
3. KH discussed and confirmed with LR the "No Lobby Bypass" policy to be default for future meetings, advising EC of this change of action.
4. KH raised awareness of the issues surrounding the bot at weekly Academic Partner ICT catchup and agreed to share recommendations with the partnership.
5. KH to warn staff of risks associated with similar tools and bots at "Essential Update" to staff returning Mid-August, with an accompanying News Hub post.

Closing statement:

Whilst this event was made possible due to a simple human error, that error was brought on by a misapprehension of the use and settings of the Microsoft Teams application. KH will work with UHI Unified Comms to produce robust guidance material applicable to all UHI Partner staff to further reinforce risks associated with AI tools and the importance of security-aware vigilance. EC and others present in the meeting of 27/5/25 acted appropriately and swiftly to address the risk of the uninvited guest. Similar situations have arisen in other meetings whereby an unverified account is seen to join a meeting (or attempt to do so) and have been removed from those meetings by participants or meeting organisers. This is often a simple error on behalf of staff joining a meeting from personal devices utilising personal Microsoft accounts. We always advise staff to ensure they use their UHI accounts for any business activity.