CYBER GUIDELINE DOCUMENT

Electronic Conferencing

ABSTRACT:
This guideline provides the policing community with advice on the use of communication software

ISSUED	DECEMBER 2024
PLANNED REVIEW DATE	NOVEMBER 2025
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements for electronic conferencing.

Introduction

As technology advances and we operate in a digital-by-default manner, thousands of meetings now take place online every day across the policing community. In the past, many of us were accustomed to meeting and sharing information face-to-face, often in secure buildings surrounded by personnel who were already known to be security cleared.

This guideline is for everyone in the policing community to assist users in using electronic conferencing securely. It focuses on the use of Teams as the preferred product available through a PDS blueprint consumer device such as a laptop or mobile but much of the advice will be the same if using other apps such as Zoom.

It offers information on how to use electronic conferencing securely and provides some etiquette guidelines to encourage good practice.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to inform and advise the policing community on the most secure communication mechanisms available to them for electronic conferencing at the OFFICIAL level and to provide sensible advice on their operation, along with appropriate etiquette for their use.

Audience

Primarily, members of the policing community of trust, those who use PDS Blueprint consumer products, and their stakeholders who interact and communicate with the policing community should be aware of this guideline.

The following groups should also be aware of the content of this guideline to ensure appropriate use within policing:

- Information Security Officers and Cyber Risk Practitioners and Managers
- Auditors providing assurance services to members of the community of trust

Finally, due to policing's reliance on third parties, suppliers acting as service providers who may be developing products or services for PDS or policing should also be made aware of and consider the content of this guideline.

Scope
This guideline applies to all users within the policing community who use electronic conferencing technologies such as Teams, Zoom, Chime, and Webex for electronic conferencing, as well as voice over internet protocol (VoIP) for calls.

Guidance

Is Teams secure for routine police business needs?

Yes. The use of Teams on any PDS Blueprint consumer device with an email address using the @police.uk domain is secure up to the OFFICIAL – SENSITIVE classification for electronic conferencing, Voice over Internet Protocol (VoIP) calls, and data storage within Teams. It should always be the first choice for electronic conferencing and VoIP calls at this classification.

Teams should always be the primary method for communications for policing, all other platforms should be considered to be used in a cautious and guarded manner, especially if they are externally hosted.

For external meetings at the OFFICIAL classification with individuals outside the policing community, Teams should be used for electronic conferencing calls. It includes built-in technologies such as certificates and security protocols to prevent eavesdropping. Further guidance can be found in the etiquette section.

Is Zoom secure for our business needs?

Zoom was very popular at the beginning of this decade when other secure and embedded platforms were not available. Free and Pro accounts have the region where their account is provisioned enabled and locked, with Pro accounts able to adjust other regions. Typically, new accounts are provisioned in the United States, meaning the United States data centre cannot be disabled. Additionally, it's research and development has been in China. Zoom may be used for meetings with the commercial / private sector if Teams is not available and/or in exceptional circumstances. Participants must carefully consider and be more guarded about what they say or share on Zoom calls whether using the application or web versions.

Is Skype and Google meet secure for our business needs?

As above, typically data centres and new accounts are located and provisioned in the United States meaning the USA data centre cannot be disabled. Additionally, other providers could be used for meetings with the commercial / private sector if Teams is not available and/or in exceptional circumstances. Participants must carefully consider and be more guarded about what they say or share on Skype or Google meet calls whether using the application or web versions..

Is Cisco Webex secure for our business needs?

Webex comes in different flavours such as Webex Government. Generally speaking, it is acceptable for OFFICAL conversations however the residency of data can vary and could be outside of the UK or EU and should be used with caution in the same way as Zoom above.

Secure Use

People need to be aware of their responsibilities to maintain the confidentiality of sensitive data if they are working remotely or travelling such that their communications may not be overheard, overlooked or otherwise noted. There is a responsibility to ensure protection against eavesdropping - either via the presence from unauthorised personnel or video or microphone functionality on non-official devices that are active in the vicinity.

Virtual assistant technologies, such as Alexa, Siri or Google Assistant, are ubiquitous and often enabled by default, they can also be embedded in any 'smart' technology devices such as TV's and wearable technology. Consideration should be given to where they are placed in relation to where work conversations are held. This is particularly important if sensitive conversations are to be held. **Users should not have such technologies active, in the same room where they routinely work.** This is primarily because they are always listening, and sensitive conversations could be captured and stored outside of policing systems. Additionally, they can cause unpredictable distractions, such as notifications during Teams calls or weather and delivery notifications.

Local secure remote working policies should be inclusive of controls to protect the confidentiality of sensitive information.

When working remotely or on the go, consider your location when taking or making a Teams or VoIP call. This may depend on who is on the other end and whether or not you will contribute to the call. If you are in a public space, be mindful of who can see your screen and whether others may be able to read the chat on your screen. Ideally, position yourself so that no one can see your screen or hear your conversation. The use of headphones is always recommended. Consider using a privacy screen cover.

Meetings created in Teams can be forwarded by guests by default. There have been instances where a meeting was inadvertently forwarded to an Artificial Intelligence technology, which then attended and started to record and transcribe the call. You can prevent forwarding in the response options dialog box before sending the meeting invite. Meeting participants should always check with the host before forwarding a meeting invite to another person and explain why they plan to do this, ensuring the host is always aware of all participants.

Meeting hosts are responsible for defining meeting expectations. This should include verifying the identity and business need of attendees, validating that attendees are not 'bots' or 'AI attendees', keeping the classification of the meeting content appropriate for attendees.

Some conferencing systems have experienced unwanted disturbances by intruders, particularly where invitations are open to a wide audience. This has been termed Zoom bombing in the media. Although less frequent than previously, such incidents do still take place. Consider how to respond to such an incident; take screenshots or screen recordings of the participants in the call; consider recording the intrusion if doing so will not put you at risk; If you can identify the intruder, you may be able to remove them from the call; have a plan for closing the conference call early and contacting an appropriate ICT Security team to raise a security incident.

Etiquette

The boom in electronic conferencing use began at the start of this decade as the world dealt with the COVID-19 pandemic. There was a great emphasis on delivering under such extraordinary circumstances, and as a result, it has changed the way we work.

Electronic conferencing is an essential tool, allowing us all to work more flexibly. The following guidance is provided to help us get the best out of our meetings:

- **Introductions**: The host should consider all participants and whether it is appropriate to conduct introductions. This helps presenters understand their audience and pitch their content more appropriately.

- **Lobbies**: Only the host should admit guests from the lobby. This helps to preserve internal pre-meeting conversations and facilitate meeting preparation.
- **Punctuality**: Always arrive on time to meetings you are invited to, or within 1 to 2 minutes. If you know you will be late, it is polite to send an instant message explaining you will be joining late and whether to wait or carry on. When you do join, a simple apology in the chat will always be appreciated; there is no need to interrupt the speaker.
- **Accessibility**: Hosts should consider the needs of any guests who are disabled and may require special accommodations, such as turning on transcription for a deaf user or providing an accessible presentation in advance for blind or partially sighted users.
- **Guest Needs**: Guests with disabilities should feel confident to reach out to hosts to ensure they get the best possible experience from a meeting by setting out what they need.
- **Profile Photo**: Consider adding a photo to your profile on Outlook and Teams. It looks more professional and creates a better connection than just seeing two letters. Note that the visibility of the photo is most likely limited to the Microsoft tenant you work on; external participants are not likely to see your photo.
- **Camera Use**: It is standard to switch your camera on for all Teams calls, but you may consider an etiquette based on the number of attendees. Imagine you are at an in-person meeting and how many people you could focus on.
- **Camera Positioning**: Try to centre your image to avoid a looming effect. Consider raising your laptop with books or using an external camera if possible. A laptop stand can also help elevate the laptop. Always consider what is in the background and whether it breaches privacy and is appropriate. This is particularly important when in public areas such as when travelling.
- **Meeting Duration**: If you have a lot of meetings, consider adjusting your calendar settings to create meetings for a slightly shorter time period, so that a 1-hour meeting will end in 55 minutes. This allows a brief break before the next meeting and encourages good timekeeping.
- **Professionalism**: Attendance at a Teams meeting should be at a level of professionalism commensurate with an in-person meeting. Guests should be centred on the screen, appropriately dressed, and refrain from vaping or smoking as they would in an office meeting.
- **Background**: Use a corporate background if available or use a background blur. If using neither, be mindful of what is visible behind you, including books on shelves or personal possessions. Be mindful of whiteboards in meeting rooms which may contain sensitive information.
- **Interruptions**: Try not to interrupt others when they are speaking. There can sometimes be a lag in data transmission, which can make this worse. Consider using the raise hand feature instead.
- **Recording and Transcribing**: Only record and transcribe meetings when necessary. It is good etiquette to announce your intention to record and/or transcribe the call and give the reason why. Allow participants the opportunity to choose to drop the call or turn their cameras off if they prefer.
- **Avatars and Virtual Rooms**: Avoid using avatars and virtual rooms as they can be misleading and confusing. Users may not be aware of all the people in the room and may say things they did not intend to share.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed, and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

This document is a guideline and not mandatory, it offers useful information that forces may choose to adopt.

Equality Impact Assessment

Adapt according to Force or PDS Policy needs.

Withdrawal of existing guideline

This guide supersedes ***NPIRMT Guidance on the use of Zoom Video conferencing by Policing Updated October 2020 v2*** which should be withdrawn.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	First draft	02/09/2024
0.2	PDS Cyber	Amendments following NCPSWG review	25/11/2024

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	04/12/24

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	07/2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021