

Guidance: Zoom Video Conferencing

Information Governance

The Zoom Service

Zoom provides an audio and video conferencing application and service, allowing users to join meetings from anywhere, on any device, at any time. However, there have been security issues with Zoom. Where there is a requirement for video conferencing, MS Teams or Skype for Business should be used. There will however be situations where there is a need to attend an external meeting hosted on Zoom. The below guidance advises on what steps should be taken in these cases to help protect the Authority's information during these unprecedented times.

Guidance on using Zoom

- Only to be used when no alternate available e.g. MS Teams, Skype for Business.
- Zoom **must not** be used for meetings where personal, sensitive or confidential information is included.
- Follow the issued guidance on Video Conferencing summarised at the end of this document.
- If joining a Zoom meeting you must be signed into a Zoom account rather than joining as a guest.
- If using Zoom, register for the account using your npt.gov.uk email address rather than a personal one.
- Set a strong, unique password for your Zoom account.

Attending a meeting using Zoom

If invited to attend a meeting held on Zoom, you must assess whether personal, confidential or sensitive information will be involved. If the meeting will include those types of information, Zoom **must not** be used. As an alternative consider hosting the meeting on Teams or Skype for Business and inviting the external parties instead.

Once you are satisfied that you can attend the Zoom meeting, you should join using the "join from your browser option". The smartphone app or the desktop application should not be used.



- When joining a meeting you will need to sign in to a Zoom account. This account should not be a personal one.
- When creating an account to attend a Zoom meeting use your npt.gov.uk email address to register.
- When attending a meeting edit your display name by right clicking on your ID in the Participants panel. You should edit this to include your name and role rather than your email address or any other identifying information.
- Be aware of who the other participants in the meeting are, particularly if people join during the meeting.
- Be aware that meetings can be recorded by the host and potentially attendees depending on their configuration. This is also the case for text chat, including private one-to-one text conversations.

When to use video calls and meetings

Video calls and meetings are valuable tools in achieving our goals and maintaining contact. There is however a balance to be struck between use and over use. One-to-one video calling can help combat social isolation, whether you are a manager checking in on how your staff are doing, or calling a colleague to discuss an issue. It can go some way to replicate the social interaction of popping to the office next door to clarify something. But you can have too much of a good thing. Over use of video calls or meetings can cause people to disassociate from the content of the meeting and reduce the usefulness of the interaction. To avoid this:

- Use audio calls unless video is needed.
- Be deliberate and clear about why you're having the meeting.
- Have as few people involved as necessary to achieve the goal.

Confidentiality for staff

1. Avoid having other people in the room with you while making video calls including children, partners or other family members.
2. When using video conferencing in an office, any visible confidential data should be removed and checked in the camera preview before starting the call.
3. If using video conferencing with external contacts or service users it is also advised that you have a neutral background which provides the participants with no clues about you or your location. The virtual background option in Zoom can help however it isn't flawless, it is advisable to place the camera to minimise any issues. Make sure you are familiar with these settings before beginning a call with external contacts or service users.
4. If sharing your screen, make sure your email, open documents, browser windows and systems such as VISION and SSIS are not shared. Preferably these would be closed to prevent accidental disclosure.

Further information on video calling can be found in the Video Conferencing Helpsheet.

Please note: Zoom must not be used for confidential or sensitive communications.