**You’re invited to a Zoom meeting**

The council and its officers have legal responsibilities for personal data from the point it is shared, through transit, and until that information is received by the recipient, including for verbal transactions, like those through video conferencing.

The council also has safeguarding and moral obligations to protect our residents, clients and staff, where we can, from illegal and upsetting incidents.

If you must attend a meeting hosted by another organisation on Zoom, such as a hearing or panel meeting, you must follow these instructions.

**Before the Meeting**

|  |  |
| --- | --- |
| [ ]  | We expect staff to **only join** meetings hosted on **paid for** (Pro Business or Enterprise) Zoom subscriptions. Check this with the host in advance.Speak to your manager immediately if a free Zoom account is being used, as your Chief Officer and the council SIRO will need to approve you joining the meeting. |
| [ ]  | Only join Zoom calls through a web browser. **Do not create a free account.** Do not click on meeting acceptance links or open attachments within any emailed meeting invitation which is not expected. A tactic of cybercriminals is to send fake meeting invitations to entice users into clicking on malicious links and opening malware infected attachments. |
| [ ]  | Find out whether the host plans to record the Zoom call and why. Discuss with your manager if you have concerns about recording. |
| [ ]  | Do not share the meeting ID or password with anyone. Ask the host to provide login details to them directly if you want another person to attend. |

**During the meeting**

|  |  |
| --- | --- |
| [ ]  | The host should ask participants to introduce themselves to help ensure that only those invited are in attendance. Stop the meeting if at any point you are unsure about who else is present. You can challenge individuals or ask the host to take a further roll call if necessary. The meeting host can send participants back to the waiting room during the meeting until identity concerns are resolved. |
| [ ]  | If a meeting organiser has turned recording on, you can ask that it be stopped, and if it isn’t, decide if it is appropriate to continue with recording turned on or leave the meeting. |
| [ ]  | Do not share documents through Zoom during the call. These should be shared securely through usual means. |
| [ ]  | If a link pops up with an attachment, do not open this unless it is something that you are expecting from the meeting host or other attendee. If you are unsure, ask the host during the call whether they have sent the attachment. |
| [ ]  | **REPORT any suspicious activity or incident** that happens during the meeting to data.protection@barnet.gov.uk as soon as the call is over. |

**Hosting Meetings or Events with Zoom**

Officers are expected to use MS Teams or Skype, as these are corporately approved apps. MS Teams is now readily available for many staff and IT are working through a priority list of services to support the configuration and set up of Teams video conferencing where appropriate. Speak to IT if you need assistance.

Service areas must show that Skype or MS Teams cannot fulfil their requirements before seeking to use other tools, such as Zoom. If you cannot use Skype or Teams, you will need to request a policy exception before you use Zoom.

Complete the request form, which must be approved by your Chief Officer. It is important that you leave enough time to make the request and comply with the criteria below for hosting through Zoom.

*Zoom is not a corporately supported application so IT will not be able to support you in set up or use.*

**Mandatory requirements**

* Only host using paid for (Pro Business or Enterprise) Zoom subscription. **You must not use a free account.** Choose the subscription that **excludes** processing in China.
* Only use a laptop approved by IT for Zoom hosting, these should be labelled. **Do not** use your normal work laptop or personal equipment.
* Use a strong and separate password for your Zoom account.

**Before the Meeting**

|  |  |
| --- | --- |
| [ ]  | There must be a minimum of 2 officers on the call:1. Acts as host, by facilitating the call, managing the Zoom settings and attendees.
2. Presents/leads the content.

Test the meeting before going live. |
| [ ]  | Do not use the Personal Meeting ID (PMI) that Zoom may create for you. You must create a Unique ID instead and a password. These must be different for every Zoom call, even if it is a recurring event. This helps to secure the meeting from intrusion. |
| [ ]  | Create an Invite Only call by using Authentication Profiles.Only send meeting invitations, Unique ID and password to those necessary to attend the event. Ask attendees not to share the meeting ID or password. Anyone wishing to join the call should register with the host in advance.  |
| [ ]  | Use your name or role, not your email address or other identifying info, when you log into Zoom (your name can be changed by right-clicking on your ID in the Participants panel and clicking “Rename”, making sure all participants use their real names or applicable role when using Zoom)  |
| [ ]  | Do not record meetings. If you need minutes, these should be taken by hand in the usual way. |
| [ ]  | If information is required by meeting participants, make it available to them securely by usual means, rather than sharing through Zoom. |
| [ ]  | Prep your environment by considering what will be on show when you are on the call. Close any other applications to prevent accidental sharing, including Skype and Teams pop up notifications. |
| [ ]  | Ensure that only the host can share their screen. In advance, go to the Zoom web portal (not the desktop app) and navigate to Personal > Settings > In Meeting (Basic) and look for Screen sharing. Check the option that only the host can share.Disable the annotation feature in the In Meeting (Basics) section of your web account, so that attendees cannot annotate what the host shares. |
| [ ]  | Use the **Waiting Room** function. When participants log into the call, they see a Waiting Room screen that you can customise. They can't get into the call until the host lets them in. You can let people in all at once or one at a time, which means if you see names you don't recognize in the Waiting Room, you don't have to let them in at all. Disable “Join before host” and “Allow removed participants to re-join”. |
| [ ]  | **Disable private chat**. Open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings then click In Meeting (Basic). Scroll until you see Private chat and when the button is grey, it's disabled.From an active meeting, click on the Chat icon in the toolbar at the bottom. A chat panel opens on the right side. At the bottom, click on the three dots and decide who participants can chat with: no one, host only, or everyone. |

**Host Responsibilities During the Meeting**

|  |  |
| --- | --- |
| [ ]  | Use the **Waiting Room** function to control access to meetings. If you start a meeting and everyone you expect to join has, you can lock the meeting from new participants. While the meeting is running, navigate to the bottom of the screen and click Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.The host can remove someone from the call through the Participants pane on the right. Hover over the name of the person you want to remove and when options appear, choose Remove.  |
| [ ]  | Check that only verified people have joined the meeting and have attendees introduce themselves. Monitor attendance throughout the call and stop if you become unsure about who is present. Take a further roll call if necessary. Send participants back to the waiting room during the meeting until identity concerns are resolved |
| [ ]  | At the start of the meeting, the host should make a brief privacy statement and provide some information about the meeting etiquette.The privacy statement will state:That LBB is hosting the meeting and the purpose of the meeting.Overview of what personal data is permitted to be discussed (in general terms) and/or confidential information.With whom the information from the meeting can be shared.Consider asking participants to put their microphone on hold if they are not intending to speak. This reduces background noise.Be aware of the presence of voice recognition technologies such as Siri and Alexa when using video/audio conferencing. The ‘always on’ nature of their operation could result in audio from conferences being uploaded to Cloud systems. |
| [ ]  | **Disable Someone's Camera**Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the Participants panel and click on the video camera icon next to the person's name. |
| [ ]  | **Prevent Animated GIFs and Other Files in the Chat**In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs. Disable file transfer to stop this. For your own meetings, open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll down a little farther until you see File Transfer and disable. There more options for exactly how to disable file transfer for certain meetings or certain groups. |
| [ ]  | **Mute participants**The host can mute and unmute an individual or everyone on a call through Manage Participants at the bottom of the Zoom window. The Participants panel opens, and you can individually mute people and disable their cameras by clicking the microphone or camera icon next to their name. The option to mute everyone at once is at the bottom of this pane.Mute upon entry. You can also mute everyone automatically when they join a call. Before the call starts, go to the web portal and navigate to Settings > Meetings and choose the meeting. At the bottom of the screen, click to Edit the meeting. Look for Meeting Options and check the box next to Mute participants upon entry.If you didn't set it up ahead of time, you can still mute people upon entry when you start the meeting. In the same panel shown above, look for the More option. Click it and choose Mute participants upon entry. You'll also see an option here to let participants unmute themselves if you want people to be able to speak up or ask questions at an appropriate time. |
| [ ]  | Ensure you have actively closed the Zoom call and disabled screen sharing when you are finished to prevent accidental sharing of your desktop activity. |
| [ ]  | **REPORT any suspicious activity or incident** that happens during the meeting to data.protection@barnet.gov.uk as soon as the call is over. |

This guidance is taken from the Cabinet Office Government Digital Service Guidance on using Zoom, as well as an article in PC Mag (How to Prevent Zoom-Bombing

By Jill Duffy 16/04/20 <https://uk.pcmag.com/how-to-work-from-home/125678/how-to-prevent-zoom-bombing>)