The Four Parishes Safeguarding Team

Safeguarding during Zoom Meetings

This guidance is based on a number of sources including guidance from Church of England National Safeguarding Team 'Using Zoom for video meetings with young people'. Another source of useful information is https://www.safeguardinginschools.co.uk/live-meetings-with-zoom/.

Overall safety considerations

Before the first Covid-19 Lockdown in March 2020, few people had heard of the Zoom video-conferencing app. Because a basic subscription was free and Zoom had more functionality for multi-person calls than familiar apps, such as 'Skype' or 'Facetime', the number of people using it grew exponentially. In March 2020, Zoom added 2.22 million users worldwide, which was more than in the whole of 2019!

The Zoom developers were not prepared for the security challenges which arose as a result of the totally unexpected growth. Back in March, it was really easy for 'baddies' to gate crash a Zoom meeting and disrupt it in a number of different ways, with the result that Zoom got a reputation for being insecure.

Zoom worked hard to improve the security and 'user interface' issues and on 8 April 2020, the company issued the first of several major upgrades, which addressed all the basic security problems. Administrators now have a number of tools at their disposal to ensure safe use of Zoom and this document lays out the guidelines that we have adopted for meetings hosted via the Four Parishes Admin Zoom account. In enforcing these guidelines, the role of the Administrator, who acts as the meeting Host, is key. Although a Host can assign any participant as a Co-Host, all meetings must be set up, opened and closed by an Administrator acting as Host. The Host is responsible for ensuring that meetings are set up with the correct parameters and that the security guidelines are followed throughout the meeting.

What risks are we safeguarding against?

The main risks are (a) 'gate-crashing' by unauthorised attendees (b) inappropriate one to one contact between attendees, including inappropriate private messaging (c) unauthorised sharing of personal details (d) unauthorised sharing of inappropriate material. In our Four Parishes, where the number of people attending meetings and services, is relatively small (average 25-35), and most of the meeting participants are already known to each other, the overall level of risk is low. However, we take our Safeguarding responsibilities seriously and we follow recommended policies and procedures, as set out below.

(a) Unauthorised attendees

- Use a new Meeting Room each time (ie. don't use the personal meeting ID).
- Don't advertise the Meeting ID and Password to people you don't know, e.g. on social media, with the exception of 'closed groups'.
- Set up a 'Waiting Room' (this is now default functionality on Zoom).
- Don't allow Participants to join before Host.
- *(optional)* Set up the meeting to automatically mute Participants on joining.
- *(optional)* Lock the Meeting Room after the meeting starts.
- For a larger meeting (e.g. where we expect more than 10 people), we will have two Hosts, one to 'manage the room' and the other to deal with any presentation material.

- To make things easier for the Hosts, we will encourage people to use their correct names or to adopt an alias if they wish to remain anonymous to other participants.

(b) Inappropriate one to one contact, including inappropriate private messaging

- The ability to create Break out Areas, which would allow Participants to meet in smaller groups, is not available by default on the Four Parishes Admin Zoom account.
- The Chat facility, which allows Participants to share messages with other individuals or with everyone in the meeting, is restricted by default so that Participants can only communicate with the Host and are not able to share private messages during the meeting.
- For meetings involving children, parents are required to attend with them.

(c) unauthorised sharing of personal details

- For meetings involving children, parents are required to attend with them. Parents can decide whether to have cameras on or not during the meeting. Parents should be advised that they can choose to join the meeting with 'camera off'.
- If we plan to record a meeting, all participants will be informed beforehand and given the option to switch their camera off before recording starts. Parents with children will be particularly advised to switch off their cameras.
- Meetings primarily involving children will not normally be recorded.

(c) unauthorised sharing of inappropriate material

- Screen sharing functionality is not available to Participants by default. Only the Host can share their screen. This will prevent any possibility of Participants displaying inappropriate material from their own device (a problem which did occur in early Zoom meetings)
- If the inappropriate behaviour of a Participant threatens to disrupt the meeting, the Host can mute their microphone and/or turn off their camera.

Hosts should also be made aware that there are two additional ways to manage meetings safely using Zoom tools:

Expel a Participant: in the participants menu, the Host can hover the cursor over a participant's name, and several options will appear, including Remove. Click that to remove a participant from the meeting. They are unable to get back in if the Host then clicks Lock Meeting.

Attendee On-Hold: if a crisis occurs and the people running the meeting need a private moment, the Host can put Participants on-hold. The Participants' video and audio connections will be disabled momentarily. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate this feature.

Julia Stutfield

18 December 2020