HERTFORD ST ANDREW

ST MARY'S, HERTINGFORDBURY

GUIDELINES FOR THE SAFE USE OF VIDEO CONFERENCING

May 2020

St Andrew's and St Mary's are currently using Zoom for services and other church-related meetings and gatherings.

Zoom has upgraded its security and continues to monitor it, however there is a small risk of meetings being hijacked by an anonymous person who would then be able to share inappropriate content.

It is important that best practice is followed with Zoom meetings (as well as other video-conferencing platforms) at all times.

There are a number of simple steps that can be taken to manage meetings safely. Most of these can be set as default settings, or should be adjusted for individual meetings. Those having a Zoom account used to host meetings should ensure that their settings are appropriate (if you are simply joining someone else's meeting, the settings are less important).

Actions for meeting Host to take:

1. **Always require a password when scheduling meetings** *(Settings – 'Schedule meeting')* From 5 April, Zoom has turned this on by default.
2. **If you have people joining the meeting by phone, also require a password.** *(Settings – 'Schedule meeting')*
3. **Don't share the password or meeting ID publicly** – email it to participants and ask them not to forward it on.
4. **For really secure meetings you could turn on authentication and even two-factor authentication.** *(Settings – 'Schedule meeting' or this can be turned on for individual meetings)* For most church purposes this may be a step too far – as it may make it harder to enable people you want to join who are less tech savvy to do so.
5. **Enable the 'waiting room'.** *(Settings – 'In meeting (advanced)*' or this can be turned on for individual meetings). This will be turned on by default from 5 April. This puts people into a 'waiting room' before the host or co-host allows them to join the meeting.
6. **Prevent participants from sharing their screen** by setting the screen sharing to 'host only'. *(Settings – 'In meeting (basic)')*. You can also disable users' ability to use the Group Chat *(message to all)* or Private Chat (message to another participant), to share using the Whiteboard facility or make annotations. *(Settings – 'In Meetings (basic)')*. You can also prevent participants from unmuting themselves if you wish to do a webcast with no verbal participation.
7. **Have someone who is responsible for managing Zoom** *(who may be different to the person leading the meeting)*. If you have set up the ability to have co-hosts *(Settings – In Meetings licenced accounts only)*, the host can share this function with another participant

once they have joined the meeting *(click on their name in the manage participants tab, and click 'Make Co-host')*. They will then have access to the 'Manage Participants' screen, and can admit participants from the waiting room, mute or unmute them. You can also temporarily put them on hold, back in the waiting room or even remove them from the meeting should that be necessary.

Suggested actions for Participants

1. **Use their name to log in** – rather than 'Ipad', for instance. This allows the meeting host to see who is coming into the meeting.
2. Consider whether you wish to create a **separate login using your email**, rather than login with Facebook or Google ID. Using these IDs can enable data sharing between applications.
3. One of the main security risks of Zoom is **phishing** (e.g. spurious emails posing as Zoom invitations, posting malicious links in Zoom chats etc.), so users ALWAYs need to remember to be careful of what links they click on and what info they give out, whatever the platform.
4. Participants joining **any** video conferences should be aware of what they have in their background - make sure there's nothing confidential that can be seen (e.g. password pinned to noticeboard immediately behind them, or something clearly identifying where they live).

Video Calling with Children and Young People

Tracy Plumpton, Youth Worker for St Andrew's and St Mary's, will be taking part in weekly video chats with children and young people in small groups.

The following guidelines will be adhered to:

1. **Parents will be present** for Junior Church Zoom - children under 11 years of age.
2. **Other Leaders will be present** for Shake Zoom.
3. **Parental consent will be sought for TMM groups (young people aged 11 – 18).** Parents will be asked to fill in a consent form via email. Parents will be made aware that Tracy will be the only adult present during the video chats.
4. **Parents/carers' WhatsApp groups** will be used to send out meeting invites and notifications to ensure that the parent/carers are aware that it is happening and can set up the young people to access the session appropriately with any oversight if they want.
5. **Codes of conduct** – appropriate behaviour for leaders will be followed as you would expect in the usual youth group.
6. **Private chat** to be turned off by Tracy at the start of the meeting. Only to be used at Tracy's discretion.
7. **Sessions will not be recorded.**