HERTFORD ST ANDREW

ST MARY'S, HERTINGFORDBURY

GUIDELINES FOR THE SAFE USE OF VIDEO CONFERENCING

March 2025

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

Zoom continues to monitor its security features, however without appropriate safeguards an anonymous person could briefly share inappropriate content or use inappropriate language until removed.

It is important that best practice is followed with Zoom meetings (as well as other video-conferencing platforms) at all times and it is important that both churches exercise due care in choosing when and where to publish links for these meetings.

The 10.30am service on a Sunday has a one-click joining option on the website and Facebook. This is likely to be the case for other activities moving forward.

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).

Suggested actions for meeting Host to take:

1. **CHECK YOUR SETTINGS: It is a good idea to check your settings before holding any meetings be it individual or the Church's licenced account - particularly if you are using the licenced account, in the unlikely event that the previous host changed the settings.**
2. **If hosting a lot of meetings, ensure the meeting ID is different for each one by selecting automatically generated number in settings when generating the meeting.**
3. **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.
4. **Enable the 'waiting room' if necessary.** *(Settings – 'In meeting (advanced)*' or this can be turned on for individual meetings). This puts people into a 'waiting room' before the host or co-host allows them to join the meeting.
5. **Prevent participants from sharing their screen** by setting the screen sharing to 'host only' (which still enables co-hosts to share their screen). *(Settings – 'In meeting (basic)')*. You can also prevent participants from unmuting themselves via an option on the Security shield if you wish to do a webcast with no verbal participation.
6. **Prevent participants from recording the meeting.**

7. **Prevent participants from recording or saving the chat.** *Please note that chat has been disabled as a default but can be re-enabled if needed for a particular meeting.*
8. **Ensure the setting is set for NOT letting anyone take control of the camera.**
9. **Ensure setting for Remote Control is disabled unless required for a specific meeting. (The remote control function allows during screen sharing, the person who is sharing to allow others to control the screen).**
10. **Ensure File Transfer is disabled unless required for a specific meeting. (This function allows hosts and participants to send files, of various sizes, through the in-meeting chat.**
11. **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 and share their screen. You can also temporarily put participants on hold, back in the waiting room or even remove them from the meeting should that be necessary.

Good practice for Participants

1. **Use your actual 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).

Regular services and seasonal services

The same IDs are used each week for our 10.30am Sunday service, Breathe, Compline and Meditation and Mindfulness (Zoom changes the ID approximately every 20 weeks). A password is embedded in the link that is emailed meaning participants do not have to enter it manually when joining the service. If a participant joins without the link they have to input both the ID and password.

This is also the case for seasonal services eg Christmas and Easter.