The United Reformed Church

Using Zoom securely

Using Zoom securely – guidance for churches

Using Zoom securely

The “Zoom boom”

Zoom has become the go-to platform of choice for people to connect with one another during the Coronavirus lockdown. It is being used by individuals, families, businesses, universities, schools and the British Cabinet to host meetings and keep in touch. Zoom reports that the number of accounts has jumped from 10 million in December 2019 to 200 million in March this year.

Church use

The Church is recommending and supporting its use by members, ministers and churches during the lockdown. There are two features that make it particularly suitable:

1. Zoom allows users a fully-featured free account, which can be used for free indefinitely. Free accounts normally restrict meetings to 40 minutes, but the company appears to be operating a discretionary policy of lifting that limit for small meetings during the lockdown. Regardless, you can simply restart a meeting for another 40 minutes after your time expires.

2. Zoom has a unique Breakout Rooms feature, which allows the meeting to break into small groups for discussion. This is ideal for a wide range of meetings where it is important for people to be able to meet in a large group but also chat together in greater depth: church services, Bible studies, prayer meetings, committee meetings, coffee mornings and other social events.

"Zoom bombing"

The popularity of Zoom has made it the target of an unprecedented wave of hack attacks, which have received prominent press coverage. The most serious of these has been the phenomenon known as "Zoom bombing", where hackers will enter meetings and disrupt them by doing anything from hurling abuse to showing porn videos on their screens. You may well have seen a large number of press reports advising against Zoom, stating that it is anywhere from insecure to dangerous to have on your machine.

Security: perspective, proportion and prospect

Being a victim of Zoom bombing must be incredibly distressing. The possibility of it happening during a church service or meeting feels very threatening. The threat, however, is far less imminent

than the publicity suggests. As with all potential threats to using the Internet, our responses and actions need to be informed and proportionate. There are 4 things we need always to remember about online security when we read articles such as those circulating about Zoom at the moment:

1. Most of these articles are written to gain attention. The typical article is likely to be sensationalised.

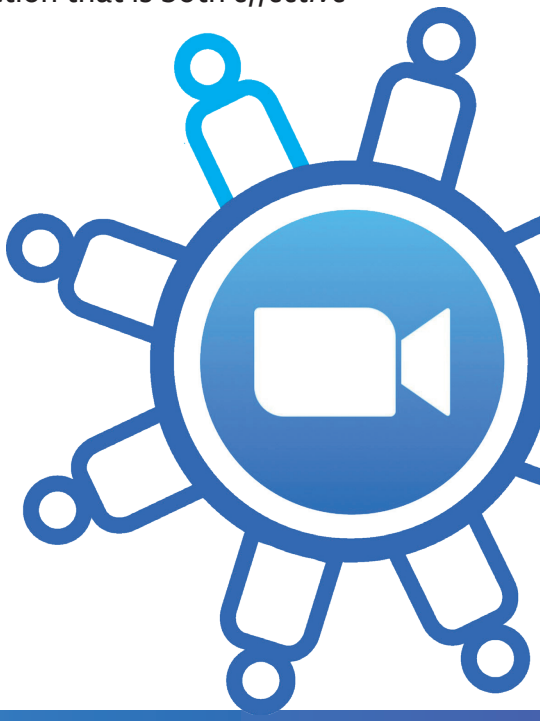
2. There is a massive difference between "possibility" and "likelihood". Think of it in terms of using medication. The manufacturers are legally obliged to include a leaflet warning you of all the possible side effects you might experience using the tablets. Most of us take the tablets none the less – because we know that the *likelihood* of experiencing an adverse reaction is almost nil. We need to read these articles in the same way. Is it *possible* that your Zoom service could be Zoom bombed? Yes! How likely is it? You are one of 200 million account holders: it is probably 99.999% the case that this will *never, ever* happen.

3. No online platform can ever be 100% safe. There is always some risk. We need therefore to take some steps to guard against the most likely risks; these need to be *effective* and *proportionate* – using what I call the *Curtain Solution*. The Curtain Solution works like this: we want to ensure that people cannot peer at will into our houses. We therefore hang curtains, which we can draw when we need to, but which are otherwise open to let the light in. We don't imagine that this is foolproof: we accept that curtains will not prevent the most determined spy from seeing in some of the time, but we don't therefore brick up the windows to make the house 100% safe

from observation! So we're looking for a Curtain Solution to using any online software platform or programme. Zoom is no different.

4. Finally, it is worth noting that Zoom is no worse than other platforms generally; it is just way, way more popular. This is why it has been the chief target for hackers. That particular cloud has a silver lining, however. Zoom has halted all development work on the roll out of new features in order to attend to security concerns. It means that we can reasonably expect Zoom to develop the most robust security protocols of any online meeting software.

The Church is therefore encouraging and supporting the use of Zoom, while issuing the guidelines that follow in order to deal with the security issues that have been identified. Churches following these will be taking responsible action that is both *effective* and *proportionate*.



Securing church services and group meetings on Zoom

Two different types of meeting

Church services and small group meetings (eg an Elders' Meeting or committee meeting) are different types of meetings and need to be managed accordingly.

Church services are public, open and accessible to all. The focus of our approach is therefore to *take action should an interruption occur*, rather than limiting access or adding additional layers of difficulty for worshippers trying to access the service.

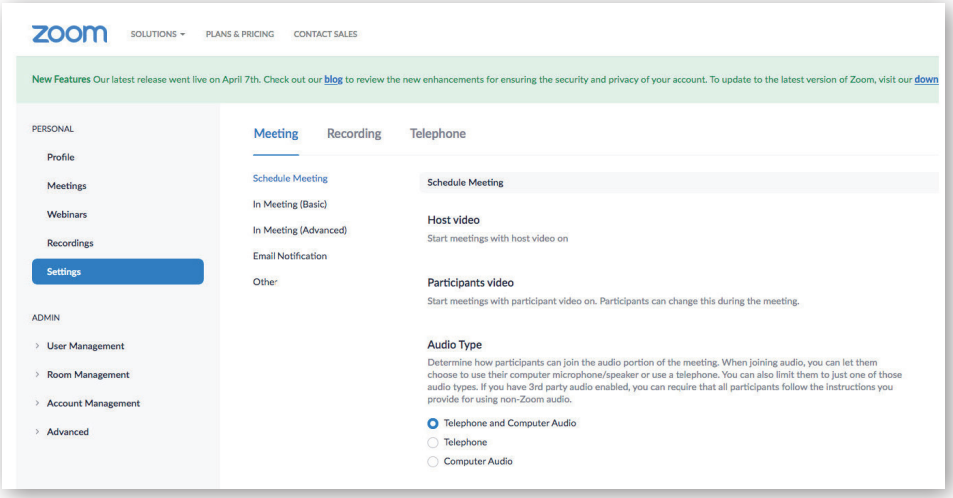
So, for example, while best practice in most settings is never to advertise a Zoom meeting ID, and always require attendees to use a password, we do not feel such measures are appropriate for a public church service.

This is no different in principle from the way in which we manage the security of our Sunday services in our church buildings. We will look at the security precautions for church services online below.

Group meetings are private, essentially invitation-only events. The approach to security is therefore to ensure that access is limited only to those people who are invited to attend. The security precautions are correspondingly different, as we shall see below.

Zoom security settings

The security settings for a meeting are set by the host and accessed through their Zoom account. To set up the meeting, go to **https:// zoom.us/** and login to your account. Click on the "My Account" tab (top right of the screen) and then "Settings". This is where you should set up your default security procedures. You can then make whatever changes you need as part of the process of scheduling a new meeting.



Here are the key recommended default security settings:

1) Join before host: disable

2) Use Personal Meeting ID (PMI) disable

One of the options for setting up a Zoom meeting is to use your own personal Zoom ID. This is often the default if you just start an ad hoc meeting. This is, in effect, a perpetual

meeting, so it is not advisable to use this room to host an open meeting because once someone has your number, they can join any meeting at any time. Instead, set each meeting up with its own ID number in the 'Schedule' menu, using 'recurring event' if necessary.

3) Require a password when scheduling new meetings: disable

Meetings can be set up with or without a password. If selected, this is a randomly generated 6 figure number. The password can be changed by you when you set up the meeting. Remember that if you change it to a word (which you can do), it will be harder for people to get in using an ordinary telephone.

You *do not* want a password for church services (hence the advice to disable this setting); you *do* want one for private meetings. You can require a password for any meeting that you set up as part of the scheduling process, so disabling this setting does not prevent this.

The pass number only comes into play if someone inputs the meeting ID number manually when joining a meeting (ie an intruder who is trying to enter without an invitation). Remember, though, that any email meeting invitation that you generate *includes* the password; if anyone outside the distribution list has access to an invitation, the password no longer provides an additional layer of security.

4) Mute participants upon entry: disable

This is not necessary for group meetings. Muting participants on entry is a good way of preventing people

entering the service and being abusive. It allows you as host to monitor who can and can't communicate.

However, entering a virtual church service full of people chatting and talking to one another is a very different experience from entering a room where everyone is silent.

Talking and interaction is one of the most important and enjoyable aspects of coming to church on Zoom – just as it is on an ordinary Sunday service at church. On the principle of dealing with issues that arise, rather than preventing their possibility, the option to mute worshippers on entry should be disabled.

5) File transfer: disable

This prevents saboteurs circulating malicious files and material to other worshippers. You will, however, need to enable it for group meetings where appropriate. Do that during scheduling; disable that feature here in your default settings.

6) Co host: enable

This is a great feature. It enables you to appoint someone as a co-host to help you monitor and manage the service. If you have enabled a Waiting Room, for example, they can admit people while you concentrate on running the service. Similarly, they can remove a troublesome attendee.

7) Screen sharing: Host Only

Use the Host Only option for both selections. This prevents a would-be zoom bomber from using their screen to share inappropriate content. This is not a necessary precaution

for a group meeting, and can be changed when scheduling a new meeting.

8) **Disable desktop/screen share for users: enable**
As above.

9) **Whiteboard: disable**
Disable this facility by default: it prevents people from writing inappropriate messages on the whiteboard if you are sharing it. You can always override this during a service or meeting if necessary.

10) **Allow removed participants to rejoin: disable**
If you have had to take the regrettable step of removing a participant, you don't want them simply rejoining the meeting!

11) **Allow participants to rename themselves: disable**
This prevents people out to cause mischief in a crowded service from "hiding" when reported.

12) **Waiting room: your call**
This can be activated when the meeting is set up, or once a meeting has been started. It is included on the 'Security' options at the foot of the screen. People only join the meeting when you admit them.

It functions somewhat like a "greeting elder" at the door of the church, and is useful as a screening process. However, it means that anyone arriving after the service has started or who leaves briefly and then returns has to be admitted before they can enter. If you want to use this facility, appoint

someone as a co-host so that you are not distracted from running the service. Or simply disable it. It's your call.

Customising meeting settings

And that's it! Once you've set your default settings, you're ready to host church services and different types of group meetings, while feeling content that you have taken the necessary steps to secure your meetings. The default settings will be applied to every meeting you schedule; you can customise them as part of the scheduling process, rather than coming back to your Settings each time.

Future updates

Remember that Zoom is working on ensuring that the software security is as robust as necessary. These guidelines will be updated regularly to reflect developments and changes. You can check the version and date of this document below. Happy Zooming!

Lawrence Moore & Revd Jamie Kissack
for the Yorkshire Synod, April 2020

This is one in a series of booklets designed to give information to those working and volunteering within the United Reformed Church.

The booklets can be read and downloaded at www.urc.org.uk/information-guides

The United Reformed Church

Produced by the Communications Team of the United Reformed Church for the Yorkshire Synod
The United Reformed Church, Church House,
86 Tavistock Place, London WC1H 9RT
020 7916 2020

www.urc.org.uk