Guide for Churches Using Zoom Securely
Rev. Stephen Allison (Kiltarlity Free Church)

Zoom is an incredibly useful tool for keeping us connected to one another in the world of Coronavirus. On the other hand, it does carry with it certain risks which have been well documented in the media. The biggest of these is the threat of "zoombombing". This is when someone infiltrates a meeting and either shares inappropriate material with everyone or disrupts the meeting in some other way. However, these risks can be mitigated against by employing the right settings in Zoom. This document is designed to give you a quick overview of the settings you should use and the practices you should employ to prevent the security issues.

1. **Know about your Zoom package**

There are different types of Zoom account – each of which has different privileges and powers.

A basic account is free and allows you to have unlimited one-to-one meetings, but for meetings with three or more people, there is a 40-minute time limit.

A Pro account is the next level and it gives the user administrative abilities such as enabling and disabling recording, and it extends meeting limits to 24 hours. If you want to employ many of the settings discussed in this document it is important that you have a Pro Account.

It is also worth noting that if you have a Pro subscription people can join your meetings by telephone but this is not supported in a basic account.

Only the person hosting the meeting needs to have a Pro subscription. Everyone else accessing the meeting can be using a basic free account.

2. **Limit how you share the Zoom details, especially on public forums**

If you share your Zoom details (Meeting IDs, Passwords etc) on a public forum such as Facebook you are more susceptible to someone accessing your meeting and causing problems.

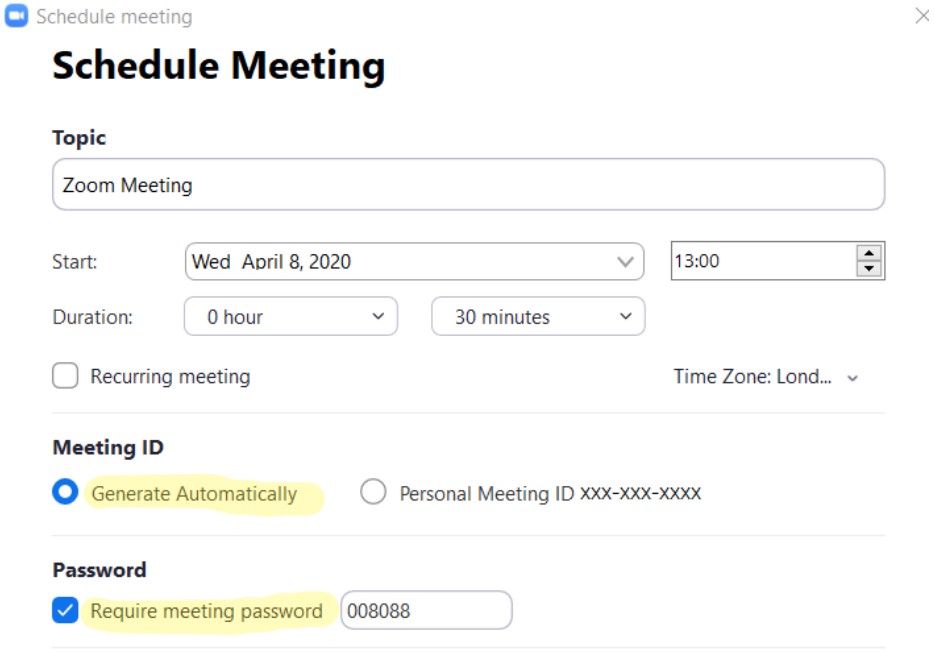
Accordingly, I would recommend that for secure meetings (such as Church Courts and Prayer Meetings / Bible Studies you should not generally share the Meeting ID or Password on social media. You could advertise the meeting but ask anyone to contact you if they wish the codes.

You may decide that it is your intention for certain meetings to be public – such as a Sunday morning service - and accordingly you want to share the details of the Zoom meeting online. That may be a reasonable decision, but you should be aware of the increased risk of infiltration and ensure other security measures are employed to mitigate the risk. I would also recommend that you have at least one co-host to the meeting who can moderate it if any problems do arise.

Kiltarlity Free Church, for example, do not share any meeting IDs on a public forum except for a Sunday service – we took this decision to encourage access to our public service. We have, however, two hosts on during the service who can remove disruptive people from the meeting and lock the meeting if necessary. We have also disabled screen sharing of participants which prevents them sharing content with others.

3. Create Randomly Generated Meeting IDs

Do not use your personal meeting ID for a public meeting – instead create a randomly generated ID. If you want to consistently use the same Meeting ID for a recurring meeting like a Sunday Service set it up as a “recurring meeting”.



If you share your personal meeting ID in public, it allows anyone who sees it to not only join that initial meeting, but to crash your personal virtual space at any time. Think of your personal meeting ID like your own phone number and then think about the privacy and security issues around sharing that number on social media.

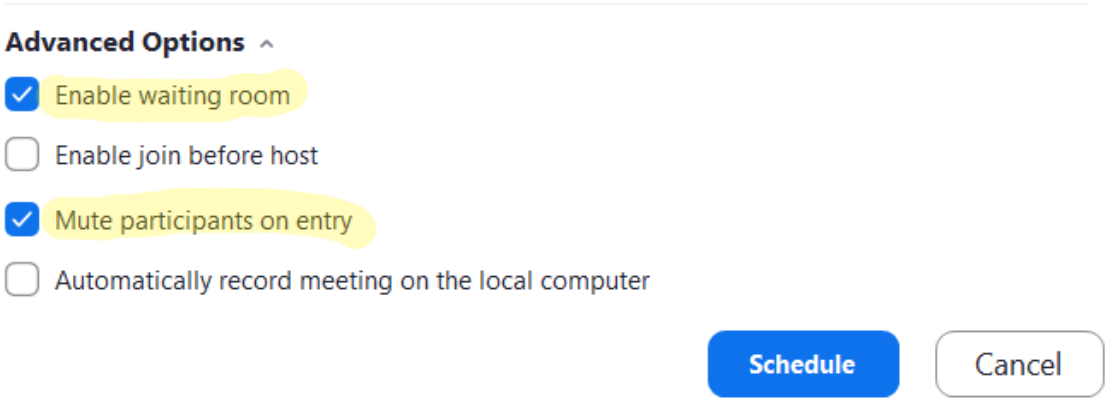
4. Set passwords on your meetings

Password protection is now being rolled out as a default by Zoom, but it’s important to ensure users are exercising this practice anyway. All Zoom meetings should have both an entry link or ID and a password in order to get in. Requiring both a Meeting ID and a password makes it harder for a hacker to randomly access a meeting.

5. Consider a Waiting Room

The waiting room is another feature of Zoom that can be enabled. It allows you to monitor who is coming into your meeting and grant them access when you choose.

When scheduling a meeting, go to your settings and click advanced options. Here you will have the ability to ‘enable waiting room’, which means that when participants do join the meeting, they will be added to a virtual waiting room, where the host of the meeting can vet participants before allowing them to join the call.



A waiting room adds another layer of security but is not essential in every meeting. I would consider using it for a more sensitive meetings – such as a Court of the Church so you can verify who is joining the call.

For further information about the waiting room see https://www.youtube.com/watch?v=ySas2Rgi6yA

6. **Restrict participant powers**

You can restrict the powers of your participants during meetings, which can often be good practice in general but, more importantly, will restrict the powers of any malicious participants.

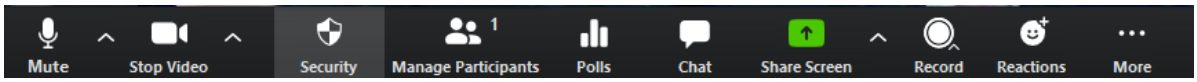
For example, you can mute all attendees upon entry to ensure that there are no disruptions. This can be done while scheduling the meeting, under advanced options in the same place you set up the waiting room, or it can be done once you have entered the meeting.

The bar along the bottom of the screen allows you to manage participants. You can mute everyone on the call or prevent them from unmuting themselves.

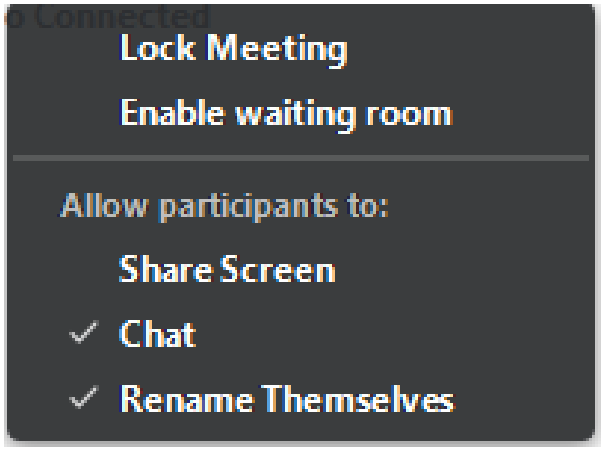
You can also ensure that only the host has the ability to share their screen by clicking the arrow next to 'share screen'. This is vital to prevent people sharing inappropriate content.

You can also restrict chat options. You can set this up to allow anyone to chat to anyone or restrict it that the participants can only chat publicly or to the host – this is particularly useful if you are running some kind of event for Young people and don't want them to be able to privately chat to one another.

These kinds of restrictions can easily be accessed in a meeting by clicking the Security button at the bottom of the page.

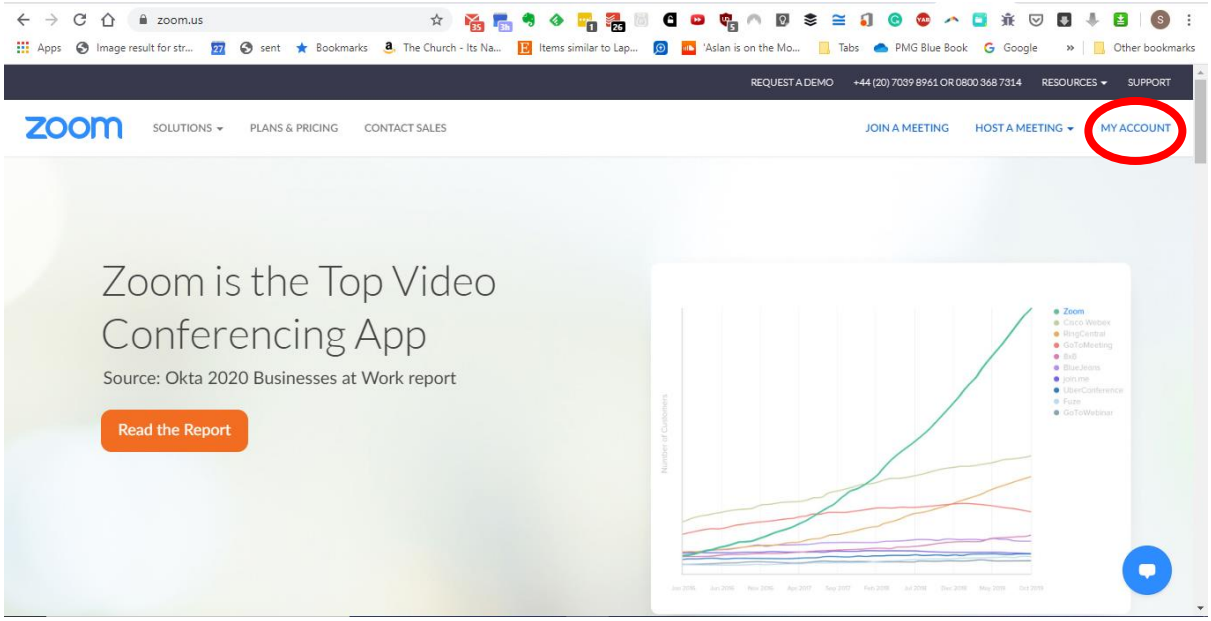


This then gives you options such as restricting who can share screen, chat or rename themselves.

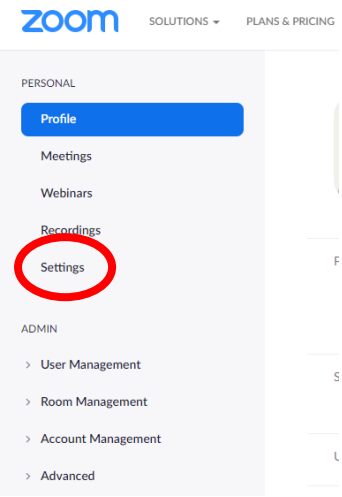


Although it is possibly to change all of these setting from within a meeting I would suggest you also look at changing some of these settings globally on your account by going to the setting page on Zoom.us. If you change the settings on Zoom.us they will apply to every meeting unless you choose to change them in the meeting.

Go to Zoom.us and login to your account. Then click “My Account”.



Then click on Settings.



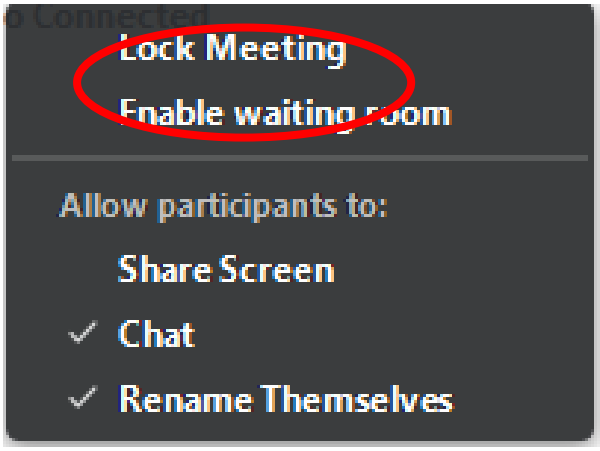
Within settings I would suggest you make the following global settings:

- Co-host (Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host) – turn this on and then you can make other participants co-hosts during the meeting.
- Screen sharing - Who can share? – set this to host only (this also allows co-hosts to share their screen).
- Annotation (Allow participants to use annotation tools to add information to shared screens) – turn this off.

7. Lock the meeting

Another helpful feature is locking a meeting once it has started as an additional security measure.

Once the meeting has started, you can select “Security” at the bottom and then select “Lock Meeting”.



This prevents anyone else joining the meeting and is a usual security measure if you are holding a private / confidential meeting. Once you know everyone is on who should be on you can lock the meeting and prevent anyone else from joining.

8. Streaming

If you are live streaming with Zoom make sure you are set to “Speaker View” rather than “Gallery View”. Speaker view will only broadcast the picture from the active window and you can fix this on one person by Spotlighting the video. Gallery View will broadcast all participants videos.

9. Alternatives to Zoom

If for a particularly private / confidential meeting you are still concerned about the security of Zoom there are other platforms available which might meet your needs for a smaller meeting.

Both Whatsapp and Google Duo offer video calls with end-to-end encryption.

Whatsapp currently allows 4 people to be on a video conference and Google Duo offers up to 12 participants.