



Using Zoom for video meetings with young people

Many churches have turned to online video-conferencing platforms to continue their ministry during the Covid-19 lockdown, including for their youthwork activities. One of the most popular platforms is Zoom. This document has been prepared to aid parishes and other ministries connected with the Church of England to understand how to use Zoom safely.

Firstly, like any other video-conferencing application, Zoom is just a tool. The general principles of safer working with young people outlined in [Safer Environments and Activities](#) should still be followed. Those principles have already been distilled for the online environment in guidance provided by the Church during the early days of the Covid-19 lockdown, which is available [here](#).

Secondly, it is important to remember that video-conferencing can be a positive way to help young people stay connected with each other and their church during these extraordinary times. We must be mindful of the risks and seek to minimise them, but we should also be mindful of the distress young people may experience if they feel isolated. By following the advice in this document, churches can continue their ministry to young people by using video-conferencing apps such as Zoom as safely as possible.

It is important to note that whilst this guidance note refers to Zoom, this is not to suggest that the Church of England is recommending the use of this particular application. This guidance focuses on Zoom as it has rapidly become very popular during the Covid-19 lockdown, and also because some security fears have been identified.

Downloading Zoom

Zoom can be downloaded from the company's website, <https://zoom.us/download>. It is vital that you only download Zoom from this site! There have been examples of people downloading versions of Zoom from other sites. Some of these versions are not safe; the best way to ensure you are downloading a safe version of Zoom is to only go to the authorised company website.

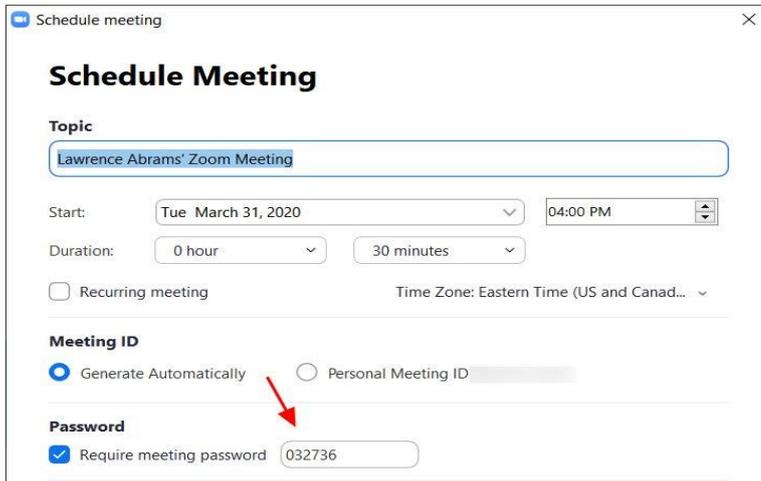
Advice from Zoom

The Zoom website has some extensive guidance, including some that has been specifically created as a response to the very rapid uptake of Zoom during the Covid-19 crisis. That guidance is available as a link from the Zoom homepage, or can be accessed directly by clicking [here](#). The guidance you are reading now is not designed to replace the guidance on the Zoom website. It is highly recommended that anyone involved in using Zoom for church ministry takes the time to become familiar with the advice on this section of the company's website. What we have provided below is advice based on some key concerns about using Zoom that have emerged recently.

Good Practice with Zoom

1. Don't advertise the Meeting ID and Password:

Each Zoom Meeting has a unique ID number and password. Give these to meeting participants directly (e.g via email or telephone), don't put them somewhere where anyone can see them (for instance, on a publicly-accessible Facebook page).



The screenshot shows the 'Schedule Meeting' form in Zoom. The 'Topic' field contains 'Lawrence Abrams' Zoom Meeting'. The 'Start' field is set to 'Tue March 31, 2020' at '04:00 PM'. The 'Duration' is set to '0 hour' and '30 minutes'. The 'Recurring meeting' checkbox is unchecked. The 'Time Zone' is set to 'Eastern Time (US and Canad...'. Under 'Meeting ID', the 'Generate Automatically' radio button is selected, and a red arrow points to it. The 'Personal Meeting ID' radio button is unselected. Under 'Password', the 'Require meeting password' checkbox is checked, and the password field contains '032736'.

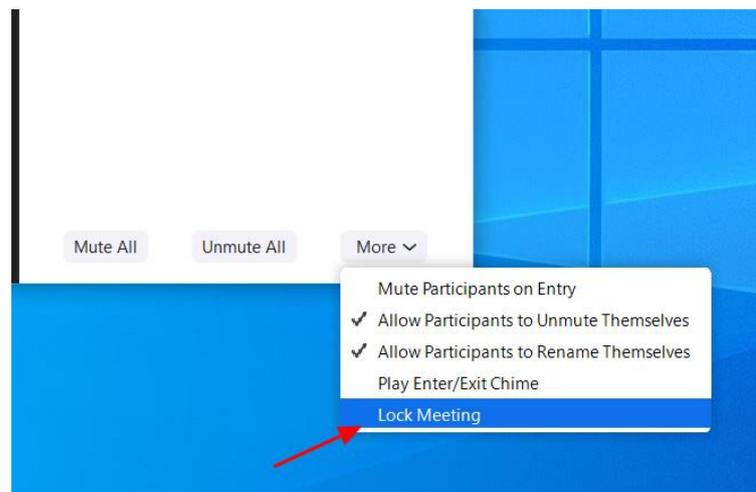
Passwords are now created automatically and will be required for every meeting; however, Zoom uses a 6 digit/character password as a default. It is recommended that you add 4 additional characters making it 10 to fall in-line with our password policy.

2. Use the Waiting Room option:

This is now a default feature but it is still best to check. When enabled, anyone who joins the meeting will be placed into a 'waiting room' where they will be shown a message stating "Please wait, the meeting host will let you in soon". The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.

3. Lock the meeting when everyone is in:

If everyone has joined your meeting and you are not inviting anyone else, you should lock the meeting so that nobody else can join. To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'MORE' at the bottom of the participants page. Then select the 'Lock Meeting' option.



4. Disable participant screen sharing:

As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options'; as shown below. When the Advanced Sharing Option screen opens, change the 'Who can Share?' setting to 'Only Host'. If the meeting requires others to share documents, send these to the host for display.



5. Know who is in the meeting:

For most situations in Church youth-work leaders will know the meeting participants beforehand, as they will be members of the youth group. As the Covid-19 lockdown progresses, however, it is possible that new people will join the youth group and want to join any video-conferencing sessions. This raises the possibility that adults who may present a risk to young people present themselves online as if they are themselves young people, in order to join such a group. Obviously the easiest way to ensure this does not happen is to use the video facility so you can see who the participants are, but someone seeking to infiltrate a group like this may, for instance, claim that the camera on their computer isn't working, or that their internet connection isn't very good so they have to turn the camera off. Remember that they will still be able to see the other participants in the meeting, even if you cannot see them. Youth leaders and others involved in this ministry in the church will need to consider how to manage this risk, ensuring that whoever is involved in video-conferencing sessions with young people is appropriate to be there. Churches may decide that only those who can turn their camera on can be involved in video sessions with young people. If this is undesirable (for instance, if it potentially excludes a vulnerable young person who would benefit from some involvement in the group during the lockdown) then a clear method of verifying the identity of the young person prior to inviting them to an online session is essential.

6. Ensure that you do not record meetings:

There is an option to record meetings in Zoom but we recommend that you turn this option off when using Zoom for meetings involving young people (and with regards to most meetings in Church). Recording meetings requires consent, and under GDPR that consent can be withdrawn at any time meaning that a recorded meeting would have to stop and the recording erased. This causes unnecessary complication and we recommend that recording is avoided unless absolutely essential.



7. Manage meetings safely using Zoom tools:

There are two other tools within Zoom that you may wish to be aware of, in particular:

- **Expel a Participant:** in the participants menu, you can hover your 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 you then click Lock Meeting.
- **Attendee On-Hold:** if you need a private moment, you can put attendees on-hold. The attendee's 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.

Sample risk assessment for using Zoom with young people in Church

Below is a **sample** risk assessment for using Zoom with young people in Church, using the risk assessment template available on the Church of England safeguarding web pages. Only one risk is identified here for illustrative purposes; you will need to identify all the risks of using Zoom and put mitigation strategies in place accordingly.

What are the hazards?	Who might be harmed and how?	What are you already doing?	Do you need to do anything else to manage this risk?	Action by whom?	Action by when?	Done
<i>Unknown people attending meetings</i>	<i>Young people in meetings whose identity may be exposed to unknown people</i>	<i>Using passwords for meetings</i>	<ul style="list-style-type: none"> • <i>Avoid making passwords publicly available</i> • <i>Use Zoom's Waiting Room feature</i> • <i>Lock meetings when all invitees are in</i> • <i>Only allow people in meetings who are using their cameras</i> 	<i>Youth Leader / meeting leaser</i>	<i>Immediately</i>	