Using Zoom In The Current Crisis

Introduction

Zoom is a useful tool, allowing the local work of each congregation to continue “virtually” online. This has become increasingly important in recent weeks when it comes to Kirk Sessions and Presbyteries continuing their ability to make decisions.

However we cannot ignore that there have been security concerns noted in the media, together with situations we have been able to create whilst testing the Zoom app and updates from Zoom themselves. Thankfully Zoom themselves have changed their default policies to stop a number of the concerns occurring in the first place but if Church of Scotland congregations or departments are to continue to use Zoom they should do so in the safest way possible. This document has therefore been devised to support that and you are encouraged to follow these instructions on how to set up a meeting.

Recording meetings

It is vital that when we set up a Zoom conference for church matters those ‘attending’ the meeting know to what extent they will be participating. For example, most people will know that their voice will be heard; for most attending they will be happy to have their video profile shown during the conference; but there might be a number of participants who do not wish their voice or video image recorded. Therefore, to comply with regulations we advise in the strongest possible terms that you should not record Zoom conferences or sessions. We have provided more technical information on why this is important towards the end of the document.

Zoom Conferences pre-scheduled prior to 4th April 2020

Zoom have recently updated their privacy settings to ensure that people need a password to join (if they are using the meeting ID) and automatically join a waiting room to be ‘admitted’ to the meeting. If you have scheduled a conference before 4th April 2020 to take place sometime in the future you should ensure that your participants know the password and that you turn the waiting room option on in your settings (see instructions below)

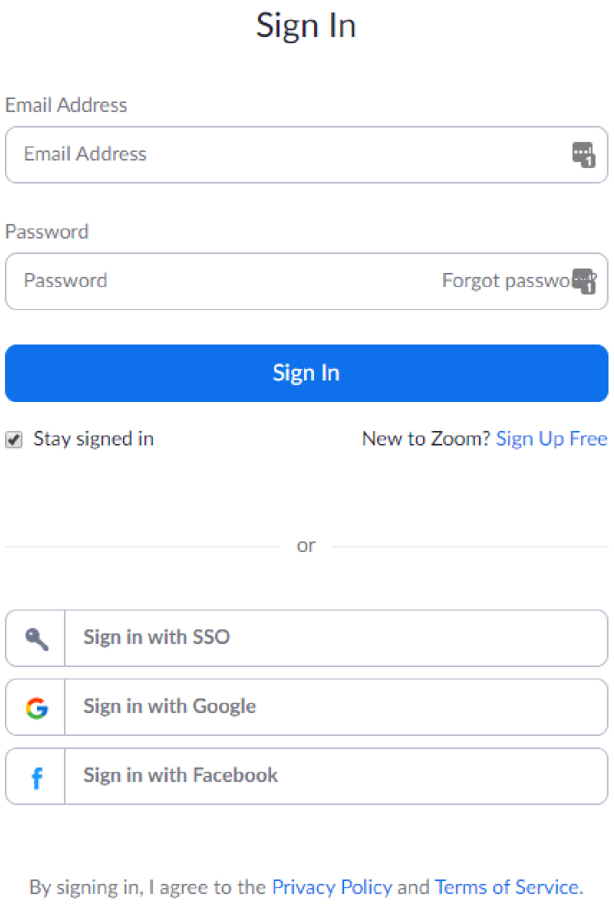
Simple steps ...

If you follow the steps contained in the next few pages when setting up a Zoom conference then you will be creating your meeting space in as secure an atmosphere as you can on Zoom. We hope that you can use them as a helpful guide to sit by your computer to aid you in your preparation.

Logging In

Log in to Zoom using an email address and password.

The advice to you is to avoid using Google or Facebook sign-in services.



Sign In

Email Address

Email Address

Password

Password Forgot password?

Sign In

☑ Stay signed in New to Zoom? Sign Up Free

or

Sign in with SSO

Sign in with Google

Sign in with Facebook

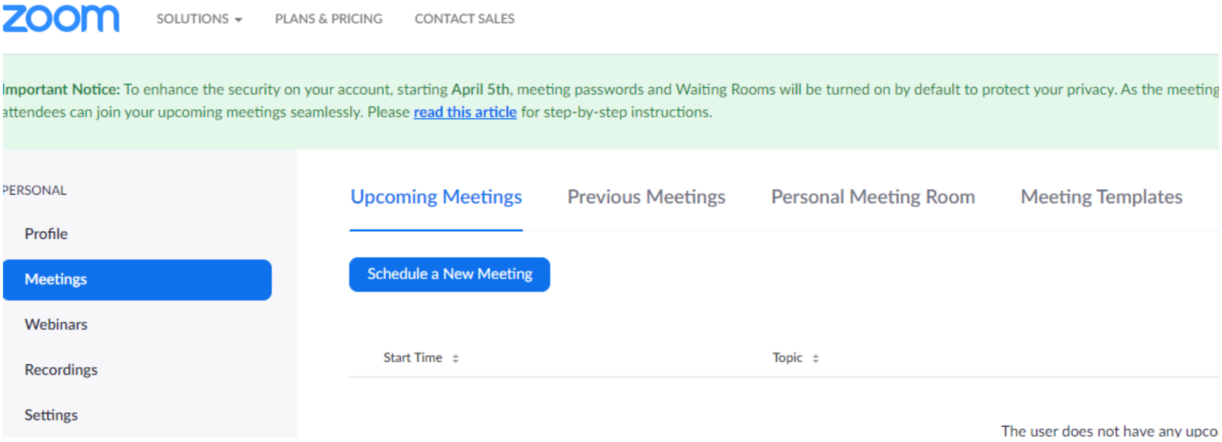
By signing in, I agree to the Privacy Policy and Terms of Service.

Profile Section

Calendar and Contact Integration: The advice is that calendar and contact integration using the Outlook Plugin or Chrome extension should not be used if it can be avoided.

The reason for this is, at the time of writing, Zoom does not offer multifactor authentication (MFA or 2FA) and therefore your user account could be compromised as a result of a phishing email designed to steal your user credentials. If this happens, there is no way to prevent unauthorised access to your Outlook or Gmail contacts lists. Remember, in the context of the Church of Scotland, this can mean unauthorised access to Special Category data.

Meetings Section

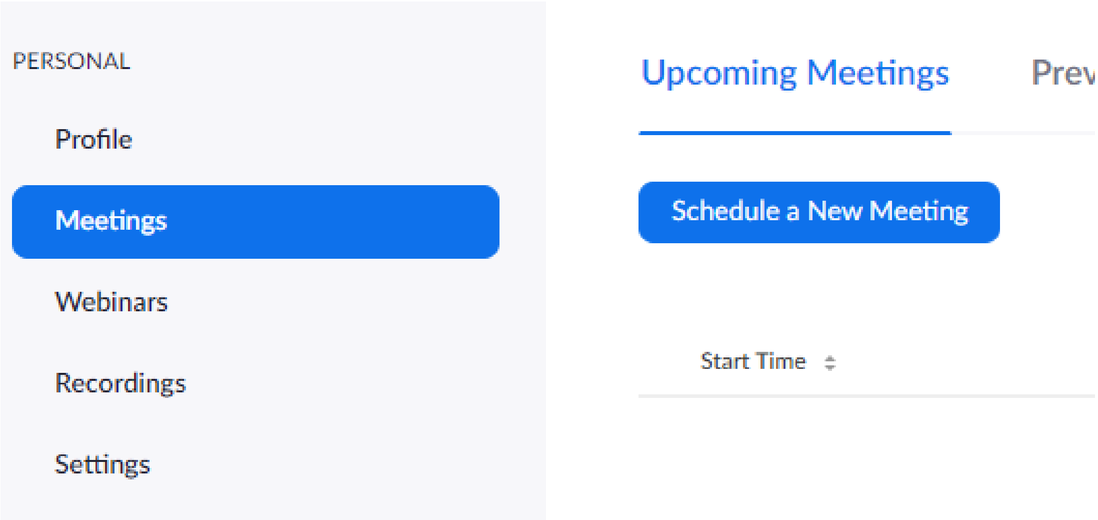


Important Notice: To enhance the security on your account, starting **April 5th**, meeting passwords and Waiting Rooms will be turned on by default to protect your privacy. As the meeting attendees can join your upcoming meetings seamlessly. Please read this article for step-by-step instructions.

The user does not have any upco

In this section, please make sure your Meetings are prepared with the following settings:

My Meetings / Schedule a Meeting



Meeting ID: GENERATE AUTOMATICALLY

Require Meeting Password: ENABLED (then choose your own password)

Waiting Room: ENABLED

Video: Host – ON, Participant OFF

Audio: BOTH (to allow users who are using a telephone to participate) or COMPUTER ONLY.

Meeting Options

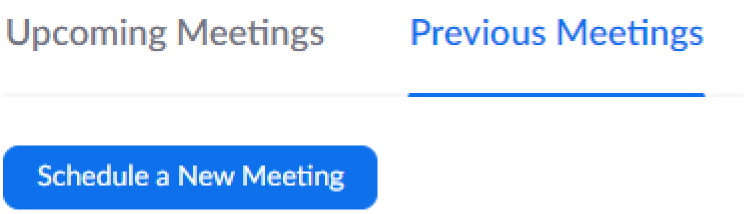
Enable join before host: OFF/UNCHECKED

Mute participants upon entry: ENABLE/CHECK for broadcast type sessions.

Enable waiting room: ENABLE/CHECK

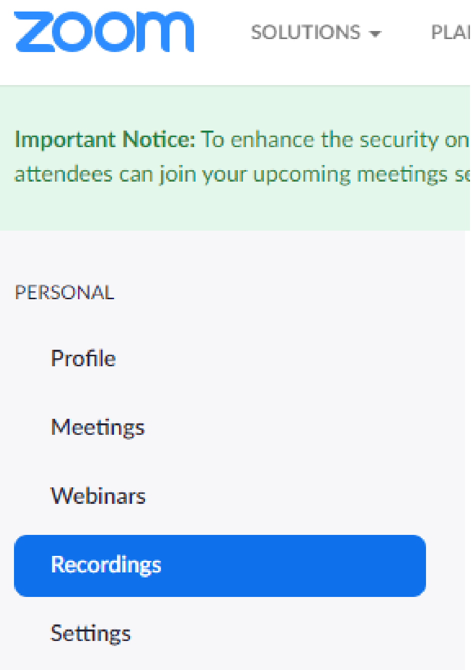
Record the meeting automatically on the local computer: DISABLE/UNCHECK

My Meetings/Previous Meetings



If you have held meetings previously and recorded them, they will be logged here. It is important that if a meeting is recorded **it is only retained for the shortest possible period of time** and then **permanently deleted.** Note that when you delete it from this screen, the recording is still available in the "Recently Deleted" page for seven days.

Recordings



Important Notice: To enhance the security on
attendees can join your upcoming meetings se

Local Recording: OFF

Hosts can give participants the permission to record locally: OFF/UNCHECKED

Automatic Recording: OFF

If meeting must be recorded: Recording Disclaimer ON

Ask participants for consent when a recording starts: ON/CHECKED

Ask host to confirm before starting a recording: ON/CHECKED

Multiple audio notifications of recorded meeting: ON

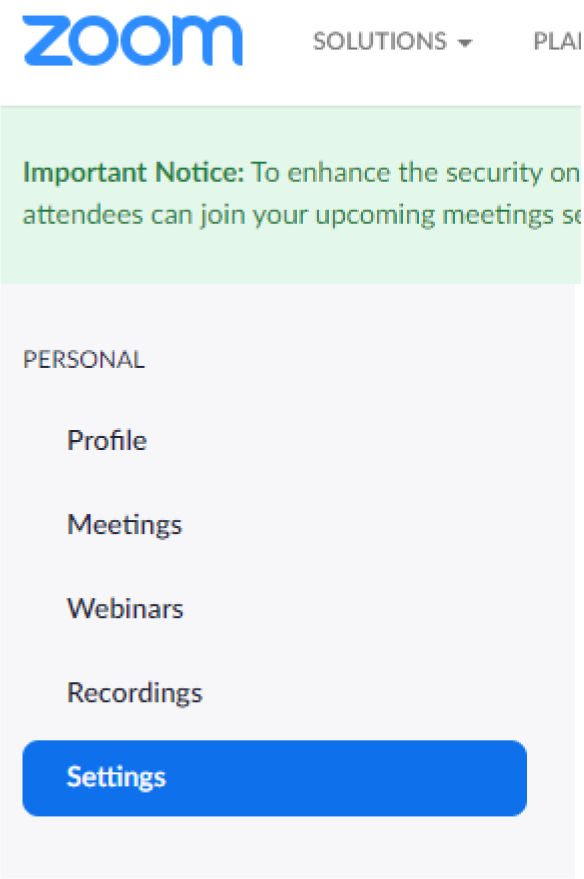
Telephone

For some of our elders and participants it is not possible to access the internet. Care should be taken when using the telephone option and you should ensure that international callers cannot call (unless you have specific need for this to be switched on, for example an elder overseas on business after this crisis is over)

Show international numbers link on the invitation email: OFF

Mask phone number in the participant list: OFF

Settings



Important Notice: To enhance the security on
attendees can join your upcoming meetings se

Host video

Start meetings with host video on: ON

Participants video

Start meetings with participant video on. Participants can change this during the meeting: OFF

Audio Type

Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio: **TELEPHONE AND COMPUTER AUDIO**

Join before host

Allow participants to join the meeting before the host arrives: OFF

Use Personal Meeting ID (PMI) when scheduling a meeting

You can visit Personal Meeting Room to change your Personal Meeting settings: OFF

Use Personal Meeting ID (PMI) when starting an instant meeting: OFF

Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client: ON

Require a password when scheduling new meetings

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included: ON

Require a password for instant meetings

A random password will be generated when starting an instant meeting: ON

Require a password for Personal Meeting ID (PMI): ON

Only meetings with Join Before Host enabled: CHECKED

All meetings using PMI: UNCHECKED (unless you are using PMI)

Embed password in meeting link for one-click join

Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password: ON

Require password for participants joining by phone

A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated: ON

Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves: ON

Upcoming meeting reminder

Receive desktop notification for upcoming meetings. Reminder time can be configured in the Zoom Desktop Client: OFF

In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H323/SIP): ON

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants: ON

Private chat

Allow meeting participants to send a private 1:1 message to another participant: ON

Auto saving chats: OFF

Play sound when participants join or leave: ON

Heard by host and all attendees: CHECKED

Heard by host only: UNCHECKED

When each participant joins by telephone

Record and play their own voice: UNCHECKED

File transfer: OFF

Feedback to Zoom: OFF

Display end-of-meeting experience feedback survey: OFF

Always show meeting control toolbar: ON

Show Zoom windows during screen share: OFF

Screen sharing: ON

Who can share?

Host Only: CHECKED All Participants: UNCHECKED

Who can start sharing when someone else is sharing?

Host Only: CHECKED   All Participants: (should not be available)

Disable desktop/screen share for users: ON

Annotation: OFF

Whiteboard: OFF

Remote control: OFF

Nonverbal feedback: OFF

Allow removed participants to rejoin: OFF

Allow participants to rename themselves: OFF

In Meeting (Advanced)

Breakout room: OFF

Remote support: OFF

Closed captioning: OFF (if you want to use this, you can change this setting)

Save Captions: OFF

Far end camera control: OFF

Virtual background: You should consider switching to OFF as part of your defence against Zoombombing

Identify guest participants in the meeting/webinar: ON

Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

Auto-answer group in chat: OFF

Enable users to see and add contacts to 'auto-answer group' in the contact list on chat. Any call from members of this group will be automatically answered.

Only show default email when sending email invites: ON

Allow users to invite participants by email only by using the default email program selected on their computer

Use HTML format email for Outlook plugin: OFF

Allow users to select stereo audio in their client settings: ON

Allow users to select stereo audio during a meeting: ON

Allow users to select original sound in their client settings: ON

Allow users to select original sound during a meeting: ON

Waiting room: ON

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.

Show a "Join from your browser" link: ON

Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited

Email Notification

When attendees join meeting before host: ON

Notify host when participants join the meeting before them (this shouldn’t happen if waiting room is selected correctly)

When a meeting is cancelled: ON

Notify host and participants when the meeting is cancelled

Other

Blur snapshot on iOS task switcher: ON

Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot display as the preview screen in the iOS tasks switcher when multiple apps are open.

GDPR and Recording

At the start of the document we stated that it is important that conferences are not recorded. Along with the fact that people ought to give their permission in advance for such a recording to take place, there is some concern over the creation and storage of recordings of video sessions. Data subjects (conference participants) involved in such recorded sessions have rights over the processing of their personal data. For Congregations and departments to be able to uphold those rights as Data Controllers, there must be both accountability for, and transparency about the recordings themselves. Each data controller is responsible for knowing and administrating the purpose of all recorded sessions, the retention period and disposal method of all recordings.

If a Data Subject Access Request (DSAR) is received after the current crisis is all over, each Data Controller (congregation, presbytery and department) is responsible for complying with the rights invoked by data subjects. If, as a data controller, you don't know where the recordings of a video session are, or you are unable to prove they have been destroyed, that will be no defence as far as the regulator is concerned.

Finally

We understand the need for the business of the Church to continue for the duration of the current crisis and by setting up Zoom conferences in with the settings contained in this document will allow you to have as much confidence as we can ever have that we have ensured the safety of all participants and upheld their rights. By applying these simple measures (and if followed step by step when setting up a conference they are simple!) we will likely avoid our own mini-crisis in a year's time.

If you have any questions please feel free to contact me.

(Allan Simpson – Data Protection Officer – The Church of Scotland)
