

The PCC of the Parish of Wiverton in the Vale

Policy: Security and Safeguarding in Zoom Meetings

Version	Date approved by PCC	Comments
1.0	18/01/2021	

What is Zoom?

Zoom is a cloud-based video conferencing service you can use to virtually meet with others - through video, audio and live text 'chats' – and it lets you record those sessions to view later. It is available through a free plan (with limited access and functionality) or a more comprehensive paid-for plan.

Zoom's core features include:

- One-on-one meetings: Host unlimited one-on-one meetings even with the free plan.
- Group video conferences: The free plan allows you to host video conferences of up to 40 minutes and up to 100 participants (with up to 49 simultaneously visible in Gallery View, dependent on device)
- Screen sharing: Meet one-on-one or with large groups and share your screen with them so they can see what you see.
- Breakout rooms: Split call participants into virtual "rooms," where they can have separate group discussions and then join back together later.

How do we currently use Zoom within the Parish?

Zoom is (or has been) used within the Parish for:

- Time for a Cuppa (online meeting following Sunday recorded services)
- Morning Prayer (on Mondays and Fridays)
- Colston Bassett Evening Prayer (Fridays)
- JOY! service
- Home Group meetings
- Parish management: PCC meetings, Worship Planning Group, Home Teams, etc.

It is hard to imagine how we might have continued to function during the pandemic without Zoom (or similar platform) and it has been used in many imaginative ways to continue to spread the Gospel within the Parish.

Most meetings are currently managed through free Zoom plans of individual members. These are limited to 40 minutes (for more than 2 participants), but any meeting may be restarted (using the same link) immediately after it has been closed, effectively allowing meetings to continue indefinitely (should you desire to do so!) with just a short break every 40 minutes.

Security and safeguarding issues

There have been a number of well-publicised security issues with Zoom, which the company has taken steps to address through updates of the software and changes to meeting options. However, by the very nature of the platform, there are still some that must be addressed by the "host" and participants of any Zoom event. A particular issue is the risk of 'Zoom-bombing', where uninvited participants disrupt the meeting with anything from verbal abuse to political diatribes or pornography. The risk of this happening in one of our meetings is small but real, so we should take sensible precautions to ensure online safety.

Zoom meetings are accessed with a knowledge of the **Meeting ID** and the **Passcode** (or a special **link** which includes these data embedded into it). Typically, these would be emailed to *bona fide* participants.

The main issue is keeping meetings accessible to anyone who has a right to be there whilst excluding anyone who doesn't. This raises the issue of who has a 'right' to be there and how invitations are distributed to such people.

For ‘worship services’, just like those which take place in church, we have a responsibility to make them accessible to anyone who wishes to join whilst maintaining the safety and security of all participants. This is a particular issue for services involving children (or vulnerable adults), such as JOY!

For ‘group meetings’, the list of authorised participants is, of course, defined by the ‘group’ and entry should be refused to anyone outside the group.

To achieve the stated objectives, the following policy is agreed by the PCC:

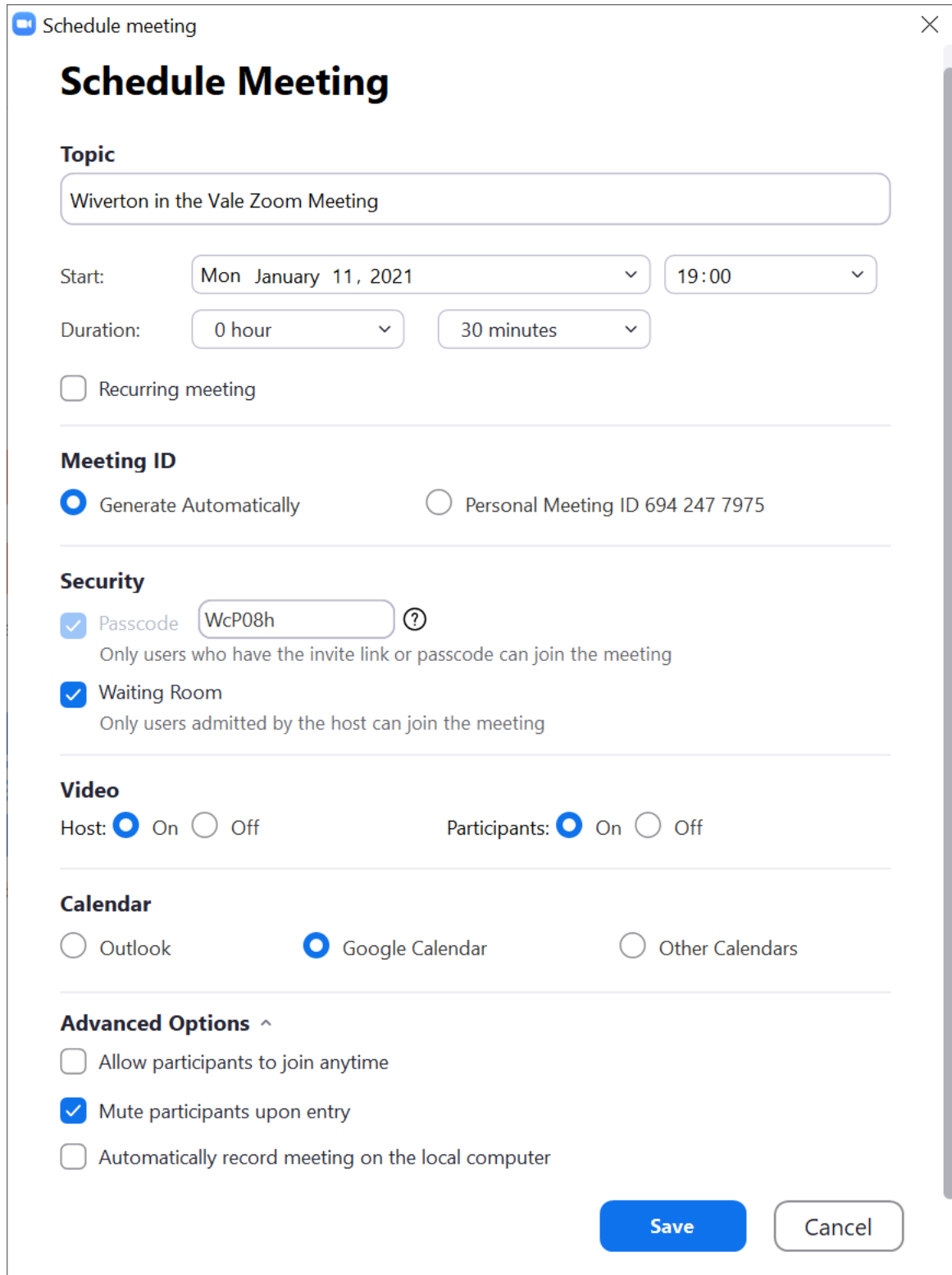
Policy to apply all Zoom meetings hosted for, or on behalf of, the Parish

Item	Policy term	Reason
1	Meetings should be scheduled in advance	Enables the prior settings of security parameters
2	Each meeting should be passcode -protected	Prevents outsiders from entering by randomly entering Meeting IDs
3	Meetings should not be ‘ recurring ’ but should each have a unique Meeting ID and passcode	If a passcode is compromised, it will only affect a single meeting
4	Participants should not be allowed to ‘ join before host ’ and a ‘ waiting room ’ should be enabled	This allows the host to vet potential participants before admitting them to the meeting
5	Wherever possible, meetings should be assigned one or more co-hosts , who can carry out administration like allowing entry from the waiting room, muting and unmuting participants, monitoring ‘chat’, <i>etc</i> , whilst the host concentrates on running the meeting	Additional layer of security to prevent unwanted visitors entering and/or contributing to the meeting
6	All participants should be muted on entry	Prevents accidental disruptions when participants enter the meeting
7	Participants should be asked to set their Display Name to their own FirstName LastName .	Identifies participants to others who may not know them personally
8	Screen-sharing by anyone other than the host or co-host should be disabled by default	Prevents participants sharing images without the permission of the host
9	Recording of meetings should not be enabled without obtaining the prior permission of all participants	Assures safeguarding of participants
10	Meeting links, invitations, IDs and/or passcodes should not be posted on any publicly accessible medium, <i>e.g.</i> websites, social media platforms	Doing so would effectively allow unrestricted access to meetings
11	Email invitations should be sent only to those: <ul style="list-style-type: none"> • who are members of the ‘group’ to which the meeting applies, or • who have requested them through a GDPR-compliant process [<i>i.e.</i> the Wiverton Updates mailing list on the MailChimp platform] which requires provision of name, address and phone number 	Restricts access to people whom we can contact by means other than email
12	People requesting invitations who are unknown to the meeting organiser (or other parish officer) should be contacted to determine their <i>bona fides</i> before they are added to the distribution list	Prevents people signing up with false credentials

How to enable the recommended settings

Clicking on the links in the preceding section will present further information about the Zoom functionality and meeting settings.

For reference, the recommended settings in the **Schedule Meeting** window of the Zoom app are as below:



The screenshot shows the 'Schedule Meeting' window in the Zoom app. The window title is 'Schedule meeting' with a close button in the top right corner. The main heading is 'Schedule Meeting'. The 'Topic' field contains 'Wiverton in the Vale Zoom Meeting'. The 'Start' field is set to 'Mon January 11, 2021' and '19:00'. The 'Duration' is set to '0 hour' and '30 minutes'. The 'Recurring meeting' checkbox is unchecked. The 'Meeting ID' section has 'Generate Automatically' selected. The 'Security' section has 'Passcode' checked with the value 'WcP08h' and 'Waiting Room' checked. The 'Video' section has 'Host' and 'Participants' both set to 'On'. The 'Calendar' section has 'Google Calendar' selected. The 'Advanced Options' section has 'Mute participants upon entry' checked. At the bottom right, there are 'Save' and 'Cancel' buttons.

Schedule Meeting

Topic

Wiverton in the Vale Zoom Meeting

Start: Mon January 11, 2021 19:00

Duration: 0 hour 30 minutes

Recurring meeting

Meeting ID

Generate Automatically Personal Meeting ID 694 247 7975

Security

Passcode WcP08h ?
Only users who have the invite link or passcode can join the meeting

Waiting Room
Only users admitted by the host can join the meeting

Video

Host: On Off Participants: On Off

Calendar

Outlook Google Calendar Other Calendars

Advanced Options ^

Allow participants to join anytime

Mute participants upon entry

Automatically record meeting on the local computer

Save Cancel

If any of these settings are not available on your screen, you may need to change some of your settings on the [Personal – Settings menu of the Zoom website](#), where these and other default meeting settings may be specified. It is worth perusing this page to see which meeting parameters can be controlled.

[Further advice on preventing meeting disruptions](#) (recommended reading for those hosting Zoom meetings) can be found on the Zoom website.