



VIRTUAL MEETINGS

A new look for Church Services and Events
Some child protection principles to consider

INDEX

1. INTRODUCTION	3
2. STAYING CONNECTED	3
2.1 CHURCH SANCTIONED	3
3. IMPORTANT PRINCIPLES	4
3.1 TYPES OF REMOTE SERVICES	4
3.2 SERVICES FOR CHILDREN	4
4. THE PRINCIPLES	5
4.2 TRANSPARENT.....	5
4.3 PUBLIC FORUM.....	5
4.4 PRIVACY PROTECTIONS	6
5. TYPES OF DELIVERY	6
5.1 LIVE STREAMING/PRE-RECORDED VIDEO OR AUDIO PROGRAMS/ACTIVITIES.....	6
5.2 VIRTUAL GATHERINGS WITH ONLINE REAL TIME ENGAGEMENT.....	6
<i>Key takeaways</i>	6
<i>BEWARE</i>	7
6. SOCIAL MEDIA PLATFORMS	7
<i>Key takeaways</i>	8
<i>Some suggestions from our limited knowledge</i>	8
6.1 SMS TEXTS.....	8
6.2 WHATSAPP	8
6.3 FACEBOOK	8
6.4 EMAIL	8
6.5 PHYSICAL CARDS/LETTERS/SUPPORT OR RESOURCE PACKS	8
7. CONCLUSION	9
APPENDIX A: ZOOM MEETINGS	10
8. ADSAFE GUIDANCE ON SETTING UP AND USING ZOOM MEETINGS	10
8.1 MEETING TYPES	10
<i>Church Leadership meetings</i>	10
<i>Church Board Meetings</i>	10
<i>Church External Meetings</i>	10
<i>Church External Meetings – with SDA Attendees</i>	10
<i>Church Public meetings</i>	11
<i>Church Private meetings – with children</i>	11
8.2 ACCOUNT SETTINGS	12
8.3 SCHEDULING A MEETING	16
<i>Outlook Plugin</i>	17
<i>Web Portal</i>	18
<i>Zoom.us app</i>	20
8.4 DURING MEETING CONTROL MEASURES.....	22
APPENDIX B: ZOOM: RESPONSE TO ONLINE CONCERNS	24
8.5 CONCERNS RAISED.....	24

1. INTRODUCTION

Overnight the look of our Australian Local Churches changed when Scott Morrison shared the decision of the National Cabinet to close places of worship. Many of our Churches were already starting to implement necessary adjustments, but it is always different when you hear it officially.

We appreciate that this has created significant change and raised some very good questions on how and what we should now be doing to continue providing a safe place where everyone can come and experience the love of God.

Please take into consideration recommendations and implement requirements from the Australian Government (with particular reference to your respective state/territory) regarding social distancing and general health when applying the following. You can keep updated here – <https://www.health.gov.au>

Currently face-to-face gatherings are not permitted which means our services have taken on a completely new look relying on digital communications through computers, tablets and smart phones. Many of our Churches are becoming very creative in how we are staying connected with our faith community and reaching out to the broader community. Many positive and uplifting aspects have come from these changes. I pray they will not be lost when we return to our 'new normal'.

With social distancing and isolating, we need to consider how best to protect and support our children and young people, while providing opportunities for them to spiritually and socially connect with Church leaders and their peers.

2. STAYING CONNECTED

2.1 Church Sanctioned

It is important for the Church Board/Leadership Team to continue to sanction/approve all programs and activities offered by your Local Church. This is particularly important for States/Territories where there are requirements for persons who work with children and where a Reportable Conduct Scheme is in operation for religious organisations. Despite the legal obligations that a church would owe the government in various jurisdictions the church leadership team are reminded of the child and vulnerable person protection policy imperatives around the conduct of persons appointed to roles by the church and to respond to any concerns raised about this conduct, regardless of whether a Reportable Conduct Scheme is presently in place. To this end the church is reminded of the principles outlined in the Church's Code of Conduct. These principles should continue to guide how volunteers engage with children and vulnerable persons in the church.

The fundamental principle that governs any organisation that provides services to their local and wider community is to assess and have a plan in place to manage the risk of harm to those enjoying these services. This task is the responsibility of the local church board or its equivalent. To this end the local church should still review its program or activities to ensure that risk of harm is properly managed. While risk of harm in established face to face programs are routinely assessed and managed within the church calendar year, this is not true of new events or events using new communication devices. The Church as an

organisation has mitigated its financial risk as it relates to child protection through appropriate insurance coverage. The church has also established a redress scheme that provides assistance for future victims of abuse within the church context, and for this assistance to be available the Church must keep adequate records around its services and events including its out-of-routine events.

register with your local conference the existence of the event under its oversight. This is important for future possible redress applicants and for any allegations of grooming or abuse.

3. IMPORTANT PRINCIPLES

As the church looks at adjusting its services in a social isolation world, there are a number of key principles for the protection of children that need to be maintained.

3.1 Types of Remote services

Table 1: Types of Remote Services

Type of Service	Examples Risk mitigation measures
Services involving Adults only	<i>Adult Sabbath schools etc</i> No Child Protection risks to manage
Wider church community services involving both adults and children	<i>Church Services</i> where children are visible in the service’s video stream or a zoom window Risk Mitigation Measure should address: <ol style="list-style-type: none"> 1. Parent approval for the child to appear in the service, and 2. Removal of any way for viewers to identify a child shown in the service. This includes deidentifying the zoom window (including either child or parent surnames)
Services specifically for Children (under 18 yoa)	<i>Pathfinders, Adventurers, Children’s sabbath schools, Virtual playgroups</i> See below for a detail description of the risk mitigation measures

3.2 Services for Children

Remote services for children create their own unique problems. These include:

1. There should already be existing restrictions around an adult’s private electronic access to other people’s children. Children are usually not online until at least 13. This may vary depending on when a parent decides that a child may have access to a smart phone. Children who are online may have regular private online communications with friends however this type of access is usually restricted for the significant non-family member adults in their life. (teachers, pathfinder leaders, counsellors, sabbath school leaders.)
2. Creating new remote online communication networks is further complicated by imperative to insist on the child protection principles that are designed to maintain

appropriate relational boundaries between children and the significant non-familial adults in their lives as contained in all adopted child safe standards evident in our community.

4. THE PRINCIPLES

These principles can be summarised as follows:

Appropriate relational boundaries between a child and the significant non-familial adults who have been appointed to leadership roles within a church community can be maintained by ensuring that all remote communication is:

1. transparent
2. in a public forum but not a public meeting
3. protects the privacy of the child

4.2 Transparent

The transparency of remote communications is enhanced by:

1. having prior approval for the service or event by the church leadership.
2. notification for the service or event is done through the parent for a child under the age of 12 or including the parent for a child over the age of 12
3. it is an agreed understanding that a parent may visit occasionally or for the duration of the service or event.
4. It is an agreed understanding that the church will have at least two child related volunteers who have completed training, signed a code of conduct and have a verified wwcc or equivalent as hosts of the service or event in one location or two.
5. Visiting adults (other than parents) may contribute to the service but only under the face to face supervision of one of the hosts.
6. Visiting Children (Children not normally part of the church group) should only be allowed to join the meeting if:
 - a) they attend the meeting physically in the presence of another child who is an existing member of the group and with the approval of that child's parent
 - b) prior approval is sought by the visiting child's parent with the agreed understanding that that parent will supervise their child at all times.

4.3 Public forum

1. No remote service or event will continue if there is only one child and one adult in the meeting. (Two adults could include one host + the parent of the child involved)
2. The virtual meeting should be recorded but the recording should remain the property of the church and not made available publicly.
3. a child should never be left alone in the same physical space as an adult who is not their parent during virtual church meeting.
4. The host of the meeting should vet the participants by using a waiting room type mechanism and once all attendees are present lock the meeting to stop any unwanted additions. A roll should be kept of all participants

5. It is an agreed understanding that parents of children attending the virtual meeting will set-up the location for the virtual meeting to be in a public location within the home.

4.4 Privacy Protections

1. The Virtual Meeting should not disclose the names of any of the child participants. Serious consideration should be given before allowing unconnected adult visitors as participants.
2. It must be an agreed understanding that all parents attending the virtual meeting will keep the identity of child participants confidential.

5. TYPES OF DELIVERY

A key to creating a safe environment for children is good screening and training of all leaders and adult helpers, transparency and the use of a public forum. Applying the principles of the Code of Conduct would still apply, noting the importance of not having one on one communication with a child in a private setting.

Currently the most popular forms of remote delivery for our child related programs and activities includes the following:

5.1 Live Streaming/Pre-recorded video or audio programs/activities

This type of delivery does not provide a mechanism for the recipient to provide a real time response and hence not seen to have a heightened risk, but the following would still be required.

1. Local Church Board or equivalent has approved the service or event
2. A recording of the program retained by the Local Church including the names of the leaders delivering the program
3. The leaders of the program (excluding guest speakers/presenters) are required to:
 - a) Be screened by the Local Church
 - b) Hold a current verified Working with Children Check (contact your local Adsafesafe Coordinator for this information)
 - c) Have completed the Adsafesafe Training (online access at <https://elearning.adsafesafe.org.au>)
 - d) Have signed the current Code of Conduct released March 2019 (can complete online at <https://elearning.adsafesafe.org.au>)

5.2 Virtual Gatherings with online real time engagement

Audio or Audio-visual mechanisms that provide the group members with the option to participate in discussions such as conference calls, Skype, facetime, Zoom meetings or equivalent options. These can be accompanied by (a) facilities to chat using individual messaging (IM) mechanism and or (b) the facility to share a screen.

Key takeaways...

- Transparency,

- **Group Communication,**
 - **A child participant's identity must be hidden**
 - **an adult participant's identity cannot be hidden, and**
 - **include parents/legal guardians**
1. When offering a virtual gathering for children in your local church the following would be required.
- a) Local Church Board or equivalent has approved the service or event
 - b) All communication to be done via a group setting with parents/legal guardians included in the communication – invite for the child to join is sent through the parents/legal guardian
 - c) No one-on-one communication with an individual child – prior, during or post the virtual gathering
 - d) Church to retain attendance records including date and names of leaders and children attending the virtual gathering
 - e) Minimum of two adults present. This may consist of:
 - (i) Two presenters of the virtual gathering at all times; or
 - (ii) One presenter of the virtual gathering (remote) and the caregiver who is physically with their child/children (or within hearing/line of sight) and understands they are responsible for their child/children at all times during the virtual gathering.
 - f) All Leaders/adult helpers of the virtual gatherings (excluding guest presenters) must:
 - (i) Hold a current verified Working with Children Check (contact your local Adsafesafe Coordinator for this information)
 - (ii) Have completed the Adsafesafe Training (online access at <https://elearning.adsafesafe.org.au>)
 - (iii) Have signed the current Code of Conduct released March 2019 (can be completed online at <https://elearning.adsafesafe.org.au>)
 - g) Only use online platforms where the identity of each member can be verified.

BEWARE

Virtual platforms are not necessarily private and there are incidences recently reported in the news where strangers with inappropriate intentions have been 'zoombombing' virtual gatherings and displaying/verbalising offensive materials/actions to children.

For further guidance on how to set-up and use Zoom meetings for church services and events please refer to Appendix A: Zoom Meetings

6. SOCIAL MEDIA PLATFORMS

These mechanisms are more likely to be used as communication mechanisms between parties in the church community rather than mechanisms to facilitate worship services or

other church events. As such these could form part of the church's communication strategy for distinct groups of community members including groups of children.

Options would include SMS texts, Facebook, Twitter, WhatsApp, Snapchat, Instagram Emailing and other similar apps where there is the option for engagement between the leader and recipients.

Note: Adsafes does not have the technical skills to provide advice in this area. You may wish to seek advice from your Conference IT support team, using the principles outlined above.

Key takeaways...

- **Transparency,**
- **Group Communication,**
- **a child participant's identity must be masked,**
- **an adult's identity cannot be hidden, and**
- **and include parents/legal guardians in all communications**

Some suggestions from our limited knowledge...

6.1 SMS Texts

Messaging communication like SMS texts should be avoided and certainly where it is just between your leader and one child.

6.2 WhatsApp

An alternative to sms is something like WhatsApp which allows:

1. A moderator to set up the group (access by invitation only)
2. Those invited only see names and not personal mobile phone numbers
3. Parents/legal guardians should be included
4. Send the child's invitation via the parents so you have parental approval
5. All communication is sent and viewed by the entire members group

6.3 Facebook

If used, ensure it is a closed set-up facebook group

6.4 Email

While young people do not generally communicate using emails, many of our schools are now relying heavily on the student email accounts so it is something that children are now checking more frequently. Once again, transparency and group communications are key – and include the parents/guardians with no one on one communication with children.

Schools rely on the email domain being school controlled and it is universally understood that each of these communications may be monitored by the school.

6.5 Physical Cards/Letters/Support or Resource packs

Some children in our church may not be able to access electronic means of communication and that is where "written communication" and support/resource packs are key to helping them stay connected. It is important to remember the key principles of our Code of Conduct. There should be no preferential treatment of one child so when sending material,

it should be the same material being shared with other children (virtual or hard copy). An added precautionary measure is to send the information to the parents/legal guardian who can then pass on and share the information with their child.

7. CONCLUSION

Our shared passion and commitment to protect and create a safe environment for children has not changed, only the delivery on how we are helping our children spiritually grow and stay connected.

Now that children are relying even more on the online world for connection, it does heighten the risk of predators making contact with them and seeking to exploit the situation to cause harm.

The online environment allows a person wishing to groom with the ability to mask who they are and have direct access to children who innocently trust the person's stated motive in the engagement.

We need to remain vigilant in our processes of screening, training and supporting our leaders and those who will now be making a connection with our children. The principles are still the same. The Code of Conduct is still relevant. Our passion to spiritually grow and help our children have a connection with God is unaltered.

As we go on this journey together, let's embrace the positive opportunities for sharing the message of our Lord and continuing to protect and support His children.

APPENDIX A: ZOOM MEETINGS

8. ADSAFE GUIDANCE ON SETTING UP AND USING ZOOM MEETINGS

8.1 Meeting Types

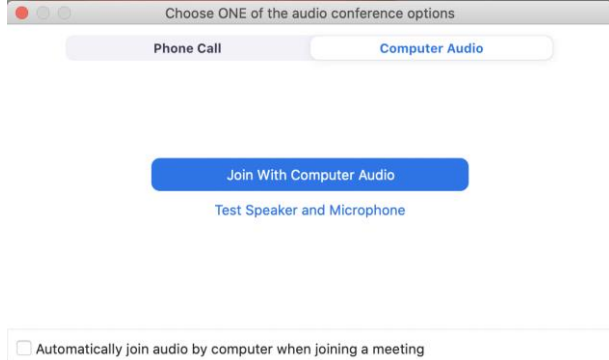





Description	Material shared	Invitees	# of People	Security Notes
<i>Church Leadership meetings</i>	Not Sensitive	Church leaders	< 15	Meeting set-up from Host account Agree understandings <ul style="list-style-type: none"> ○ all staff join with video on ○ gallery view provides comfort on participant ID
<i>Church Board Meetings</i>	Sensitive	Church Board members	< 30?	Meeting set-up from Host account Settings – set-up Meeting ID:= Generate Automatically Require meeting Password = yes Only Authenticated users can Join=Yes Settings – Meeting time Allow Participants To: Share Screen= Yes Chat= Yes Rename Themselves = No
<i>Church External Meetings</i>	Sensitive	Church Leadership Conference Leaders	< 10	Meeting set-up from Host account Settings – set-up Meeting ID:= Generate Automatically Require meeting Password = yes Only Authenticated users can Join=No Settings – Meeting time Allow Participants To: Share Screen= No Chat= No Rename Themselves = No
<i>Church External Meetings –</i>	Sensitive	Church Leadership	<10	Meeting set-up from Host account Settings – set-up









Description	Material shared	Invitees	# of People	Security Notes
<i>with SDA Attendees</i>		Conference Leaders Church members or attendees		Meeting ID:= Generate Automatically Require meeting Password = yes Only Authenticated users can Join=No Settings – Meeting time Lock meeting=yes – after all present Allow Participants To: Share Screen= No Chat= No Rename Themselves = No
<i>Church Public meetings</i>	Not Sensitive	Church Leadership Church members Members of the public Including Children	> 20	Meeting set-up from Host account Settings – set-up Meeting ID:= Generate Automatically Require meeting Password = yes Only Authenticated users can Join=No Settings – Meeting time – security icon Lock meeting=No Allow Participants To: Share Screen= No Chat= No Rename Themselves = No Host Management of Meeting From the Participants sidebar you can: Unmute or Turn on Video for a user or all Eject a person from the meeting Message a speaker Put the meeting on hold (pause everyone) Start an individual participant from hold From the chat sidebar you can (bottom "...") : Control who can chat to who Save the chat log
<i>Church Private meetings -</i>	Not Sensitive	Children’s leaders (hosts) Children	<50	Meeting set-up from Host account Settings – set-up Meeting ID:= Generate Automatically Require meeting Password = yes














Description	Material shared	Invitees	# of People	Security Notes
<i>with children</i>		Parents of Children		<p>Only Authenticated users can Join=No</p> <p>Send invite to Parents – rely on parent to log the child in</p> <p>Suggest the use of a waiting room to vet attendees</p> <p>Settings – Meeting time – security icon</p> <p>Lock meeting=Yes, Lock the meeting</p> <p>Allow Participants To:</p> <ul style="list-style-type: none"> Share Screen= No Chat= No Rename Themselves = Yes <p>Suggest that Host or parent rename each window to mask the child’s identity</p> <p>Host Management of Meeting</p> <p>From the Participants sidebar you can:</p> <ul style="list-style-type: none"> Unmute or Turn on Video for a user or all Eject a person from the meeting Message a speaker Put the meeting on hold (pause everyone) Start an individual participant from hold <p>From the chat sidebar you can (bottom “...” :</p> <ul style="list-style-type: none"> Control who can chat to who Save the chat log





8.2 Account Settings

The Zoom web portal allows a user to set the default setting for any meeting that is set-up by this user. These can be adjusted at <https://zoom.us/profile/setting>. You will need to log in first. The following table shows a selection of the settings available that are considered the most critical as secure defaults. It is understood that these settings control both the options available in the scheduling of a meeting and the default settings when a meeting is started.

Setting	Notes
<p>Audio Type</p> <p>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.</p> <p> <input checked="" type="radio"/> Telephone and Computer Audio <input type="radio"/> Telephone <input type="radio"/> Computer Audio <input type="radio"/> 3rd Party Audio </p> <p>User is given this option</p>  <p><input type="checkbox"/> Automatically join audio by computer when joining a meeting</p>	<p>User given option when joining to use a phone for audio and separate internet bandwidth for video.</p> <p>Useful if bandwidth is poor</p>
<p>Join before host </p> <p>Allow participants to join the meeting before the host arrives</p>	<p>Allow for Church leadership meetings</p> <p>Don't allow for external meetings or meeting involving children</p>
<p>Use Personal Meeting ID (PMI) when scheduling a meeting </p> <p>You can visit Personal Meeting Room to change your Personal Meeting settings.</p> <p>Use Personal Meeting ID (PMI) when starting an instant meeting </p>	<p>PMI meetings are always active and can be hijacked. Use Automatically generated meeting ID's</p>
<p>Only authenticated users can join meetings </p> <p>The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.</p> <p>Only authenticated users can join meetings from Web client </p> <p>The participants need to authenticate prior to joining meetings from web client</p>	<p>A good security measure but requires all participants to have a Zoom Account. Perhaps not something easy to explain to the general church attendee.</p> <p>Small sensitive meetings could benefit from this authentication measure. Perhaps over kill if all participants are known to each other.</p>

Setting	Notes
<p>Require a password when scheduling new meetings </p> <p>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.</p> <p>Require a password for instant meetings </p> <p>A random password will be generated when starting an instant meeting</p> <p>Require a password for Personal Meeting ID (PMI) </p> <p><input type="radio"/> Only meetings with Join Before Host enabled</p> <p><input checked="" type="radio"/> All meetings using PMI</p>	<p>Password are extra security for your meetings.</p> <p>This is enhanced if you use two factor authentication (sent link and pw separately)</p> <p>See next setting (Embedded passwords)</p>
<p>Embed password in meeting link for one-click join </p> <p>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.</p>	<p>Not much point having a password that is sent with the link or embedded with the link.</p> <p>If using the password mechanism, consider sending the password separately</p>
<p>Chat </p> <p>Allow meeting participants to send a message visible to all participants</p> <p>Private chat </p> <p>Allow meeting participants to send a private 1:1 message to another participant.</p> <p>Auto saving chats </p> <p>Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.</p>	<p>For internal meetings Chat is not a problem.</p> <p>For external meetings this should be controlled.</p> <p>Can be adjusted at meeting time by host</p>
<p>Play sound when participants join or leave </p> <p>Play sound when participants join or leave</p> <p><input checked="" type="radio"/> Heard by host and all attendees</p> <p><input type="radio"/> Heard by host only</p> <p>When each participant joins by telephone</p> <p><input type="radio"/> Record and play their own voice</p>	<p>Useful to alert the meeting participants to new attendees when they join</p>

Setting	Notes
<p>File transfer </p> <p>Hosts and participants can send files through the in-meeting chat. </p>	<p>Useful for internal meetings</p> <p>Suggest restricted for external meetings</p> <p>Can be adjusted at meeting time by the host</p>
<p>Feedback to Zoom </p> <p>Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting</p> <p>Display end-of-meeting experience feedback survey </p> <p>Display a thumbs up/down survey at the end of each meeting. If participants respond with thumbs down, they can provide additional information about what went wrong. </p> <p><input type="radio"/> Display for every meeting</p> <p><input checked="" type="radio"/> Display for meetings randomly</p>	<p>Adsafe has no opinion on this one</p> <p>You choose</p>
<p>Polling </p> <p>Add 'Polls' to the meeting controls. This allows the host to survey the attendees. </p>	<p>Adsafe has no opinion on this one</p> <p>You choose</p>
<p>Screen sharing </p> <p>Allow host and participants to share their screen or content during meetings</p> <p>Who can share?</p> <p><input checked="" type="radio"/> Host Only <input type="radio"/> All Participants</p> <p>Who can start sharing when someone else is sharing?</p> <p><input checked="" type="radio"/> Host Only <input type="radio"/> All Participants</p>	<p>For external meetings this should be set to host only</p> <p>Can be adjusted at meeting time by the host</p>
<p>Annotation </p> <p>Allow participants to use annotation tools to add information to shared screens </p> <p>Whiteboard </p> <p>Allow participants to share whiteboard during a meeting </p> <p><input type="radio"/> Auto save whiteboard content when sharing is stopped</p>	<p>Useful for internal meetings</p> <p>Should be switched off for external meetings</p>
<p>Remote control </p> <p>During screen sharing, the person who is sharing can allow others to control the shared content</p>	<p>Useful for tech support</p> <p>Should be switched off for all meetings</p>

Setting	Notes
<p>Nonverbal feedback</p> <p>Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel. </p> <p><input type="checkbox"/></p>	Should be switched off for external meetings
<p>Allow removed participants to rejoin</p> <p>Allows previously removed meeting participants and webinar panelists to rejoin </p> <p><input checked="" type="checkbox"/></p>	Normally no but if you make a mistake when ejecting a person do you want to be able to allow them to reenter?
<p>Allow participants to rename themselves</p> <p>Allow meeting participants and webinar panelists to rename themselves. </p> <p><input type="checkbox"/></p>	Stops person from hiding as a participant.
<p>Far end camera control</p> <p>Allow another user to take control of your camera during a meeting</p> <p><input type="checkbox"/></p>	Not sure if there is ever a valid reason for this?
<p>Identify guest participants in the meeting/webinar</p> <p>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. </p> <p><input type="checkbox"/></p>	Could be useful if an external consultant was presenting to a meeting
<p>Show a "Join from your browser" link</p> <p>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</p> <p><input checked="" type="checkbox"/></p>	Useful for invitees who don't have administration rights for their computer
<p>Allow live streaming meetings</p> <p><input type="checkbox"/></p>	This should be switched off for all but large Adsafes Public meetings
<p>There are many email notifications you may wish to experiment with.</p>	

It is noted that at this time of excessive Zoom usage Zoom has chosen to deactivate some of the settings that represent a privacy risk.

8.3 Scheduling a meeting

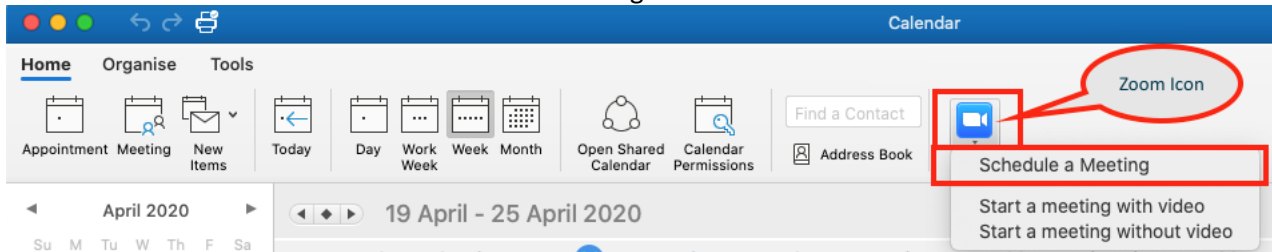
This can be done either through:

1. an Outlook plugin
2. the web portal – need to login

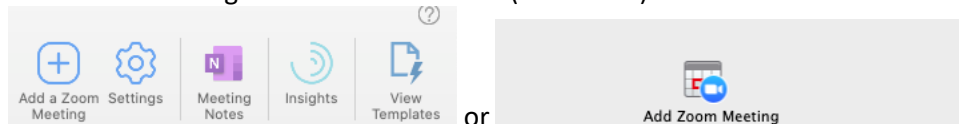
- the download Zoom app Zoom.us

Outlook Plugin

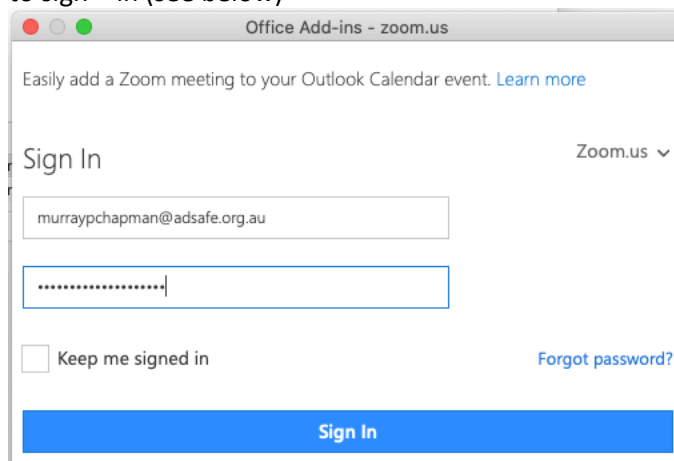
- Open Outlook and go to the calendar view. You will get following window. Click on the Zoom Icon and select Schedule a meeting.



- Alternatively add a meeting to open a meeting organiser window. You should notice the Add Zoom Meeting icons in the menu bar (see below)



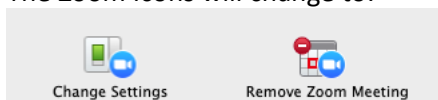
- To schedule a zoom meeting use either of the add zoom meeting icons. You may be asked to sign – in (see below)



If so sign In and select Keep me Signed In.

- You will asked to set the parameters of the meeting as seen below

5. When you are happy with the settings click Continue
6. The Zoom Icons will change to:



Which allows you to change the setting or remove the attached Zoom meeting

7. If you wish to book a zoom room for the meeting as well, search for the zoom room in the location field

Location:

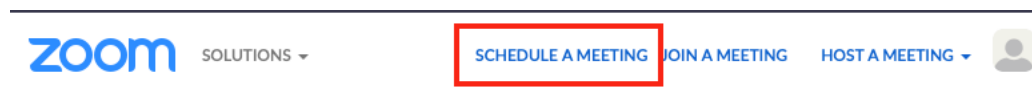
8. This will add the Zoom room to the invite list.

To:

9. Add the email address for all other invitees to the meeting into the To field.
10. The message should include the Zoom invite particulars and these will be added to the calendar event entry.
11. Type any further particulars above the Zoom invite in the message box.
12. When all is completed, send the meeting invite. This should now appear in your calendar along with the particulars of Zoom Invite and those who have accepted the invite.

Web Portal

13. Login to the Web Portal at
14. Select schedule a meeting



15. Fill out the meetings particulars as below

My Meetings > Schedule a Meeting

Schedule a Meeting

Fill out these particulars

Topic: My Meeting

Description (Optional): Enter your meeting description

When: 04/15/2020 7:00 PM

Duration: 1 hr 0 min

Time Zone: (GMT+10:00) Canberra, Melbourne, Sydney

Recurring meeting

Registration: Required

Must use these settings

Meeting ID: Generate Automatically ~~Personal Meeting ID 319 478 8889~~

Meeting Password: Require meeting password 309306

Default Value can be changed later

Video: Host on off
Participant on off

Audio: Telephone Computer Audio Telephone and Computer Audio
 3rd Party Audio
Dial from Australia [Edit](#)

Allows participant to use a phone for audio instead of the computer

16. Continue completing the meeting particulars as per below



Meeting Options

- Enable join before host internal meetings = Yes
External Meetings = No
- Mute participants upon entry Only use if you want to vet attendees
- Enable waiting room Great security measure but requires all participants to have Zoom Account
- Only authenticated users can join
- Breakout Room pre-assign Can be used to divide participants into preassigned groups - use if needed
- Record the meeting automatically Other hosts have to have Zoom accounts with the same powers

Alternative Hosts

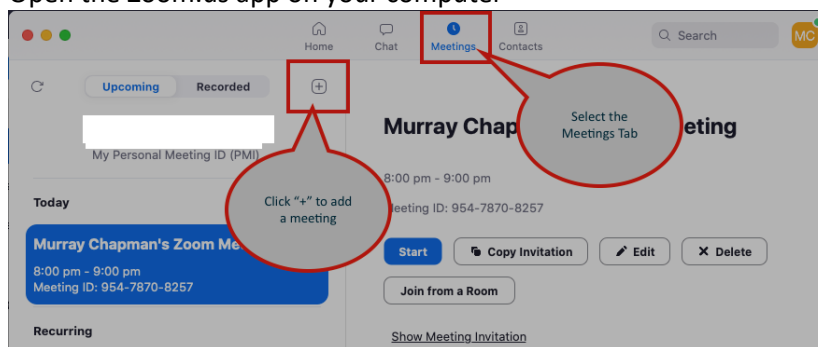
Interpretation Enable language interpretation

Save
Cancel

17. When completed and checked Save the scheduled meeting

Zoom.us app

18. Open the Zoom.us app on your computer



- 19. This should give you the following screen
- 20. Select the meetings tab and click the + icon to schedule a new meeting
- 21. This should open the following screen
- 22. Complete the form as suggested



Schedule Meeting

Topic

Complete the meeting particulars

Date
 to
 Recurring meeting Time Zone: Canberra, Melbourne, Sydney

Meeting ID
 Generate Automatically
 ~~Personal Meeting ID: 010-475-5000~~

Password
 Require meeting password

Video
 Host On Off Participants On Off

Audio
 Telephone Computer Audio
 Telephone and Computer Audio 3rd Party Audio
Dial in from Australia [Edit](#)

Calendar
 iCal Google Calendar Outlook Other Calendars

Advanced Options ^

- Enable Waiting Room
- Enable join before host
- Mute participants on entry
- Only authenticated users can join: Sign in to Zoom
- Automatically record meeting

Alternative Hosts:

Interpretation
 Enable language interpretation

See Web Portal method above for an explanation of each Item

23. Select Schedule when done.



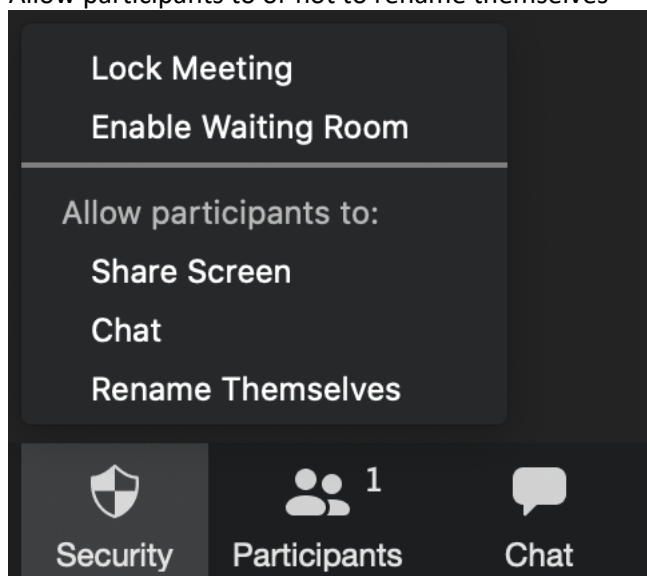
8.4 During Meeting Control measures

The host has the following controls found at the bottom of the Zoom window once the meeting as commenced

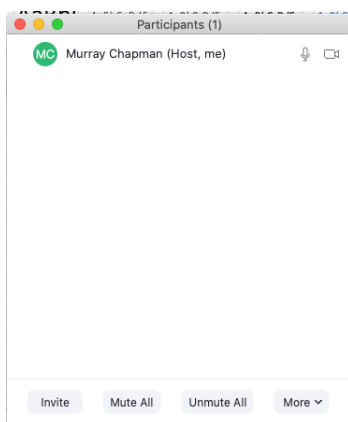


The recently implemented Security Tab allows the host to:

1. Lock the meeting – stops anyone else joining
2. Enable waiting room
3. Turn share Screen on or off for participants
4. Turn on or off chat
5. Allow participants to or not to rename themselves



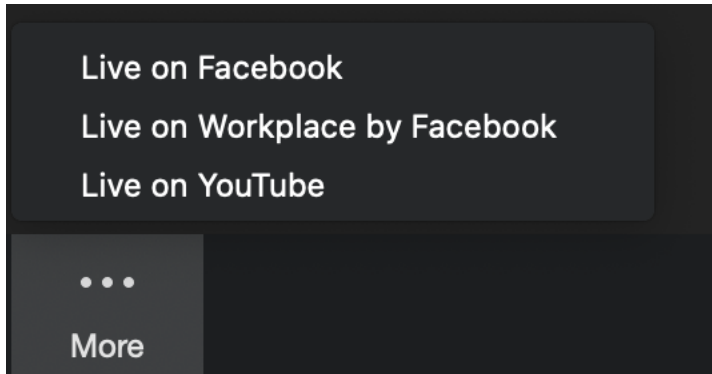
The Participants tab opens a window showing all the participants and allows the host to perform actions on individuals or groups of participants.



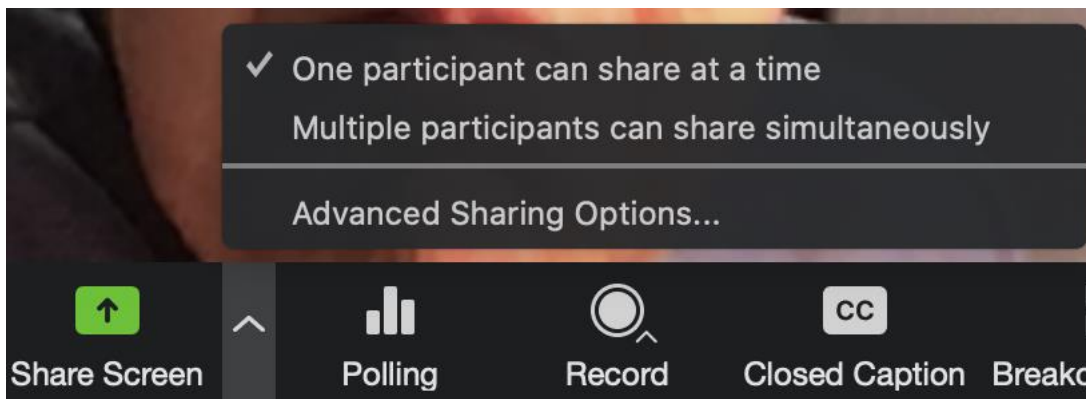
Hovering over a participant allows you to access other options



The more option at the bottom provides access to setting up live streaming on other platforms. These can be set or unset.



The sharing tab up arrow opens a menu with the following options



Each of these options can be set or unset

The Advanced sharing options opens the following window providing adjustments to sharing options



APPENDIX B: ZOOM: RESPONSE TO ONLINE CONCERNS

8.5 Concerns Raised

The following are responses to online concerns around the security of Zoom Meetings

#	Concern	Response
1	You may have heard of the recently coined term “Zoom-bombing”. There have been many cases of malicious actors joining zoom meetings uninvited , to share pornography, profanity and other offensive acts. This is enabled by Zoom’s lax security defaults, and in the past, by predictable meeting IDs . Zoom has been improving the security defaults after coming under scrutiny, but this should never have been the case.	<ul style="list-style-type: none"> • Avoid using your Personal Meeting ID (PMI) to host public events. (Meeting ID: Generate Automatically) • Control who can share screen their screens with the meeting (only host/s) • Set-up meeting to “require meeting password” and send the password separate to the invite. • Set-up the meeting so that “only authenticated users can Join: Sign in to Zoom”
2	Zoom’s claim of end-to-end encryption is misleading marketing . Their “version” of end to end encryption, allows them to access unencrypted audio and video from your meetings. True end-to-end encryption would prohibit this.	Zoom communications are established using 256-bit TLS encryption and all shared content can be encrypted using AES-256 encryption. This means that if anyone intercepts communications between Zoom Client, Zoom Room or Zoom Server the information can’t be deciphered. However the Zoom organisation can access the information from their server.
3	Thousands of users have had their personal information leaked to strangers . Zoom has a “Company Directory” setting that automatically adds other people to a user’s list of contacts, if the address shares the same domain. Many have encountered this when using their ISP provided email address. Zoom Response Domain Contacts Visibility For free Basic and single licensed Pro accounts with unmanaged domains , contacts in the same domain will no longer be visible. We’ve also removed the option to auto-populate your Contacts list with users from the same domain. If	Company Directory is available from your Zoom Account or connected to the zoom room. If a person’s Zoom Account is a corporate email address, Zoom will create Directory entries for all persons with the same domain (---@adventist.org.au) If a person uses a private email address like (xxxxx@tpg.com) for their Zoom login. The Company Directory may be a list of all persons with this domain with accounts in zoom. This problem only exists if an employee or volunteer uses their

	you would like to keep those contacts, you can add them as External Contacts.	private email address for their Zoom Account name.
4	The Zoom iOS app sent users data to Facebook , even if they didn't have a Facebook account. There was nothing in their privacy policy to address this. This casts serious doubt of the accuracy and truthfulness of their privacy policy.	If a user is using the iOS Zoom app they need to update it immediately. Zoom has now updated the app so that it no longer behaves in this way.
5	<p>There is a security flaw in Zoom chat that allows malicious links (UNC path injection) to be posted in Zoom chat. When clicked, by an unsuspecting user, malware could be installed on your device, and your device password can be leaked to the attacker.</p> <p>Zoom Response</p> <p>File Transfers The option to do third-party file transfers in Meeting and Chat was temporarily disabled. Local file transfer is available with our latest release. Third-party file transfers and clickable URLs in meeting chat will be added back in an upcoming release.</p>	<p>For private meetings agree to only type text into the chat (no copying and pasting links)</p> <p>For Public meetings only allow the host to insert text into the chat box.</p> <p>Note:</p>

Other Zoom Responses

Security Toolbar Icon for Hosts

The meeting host will now have a [Security option](#) in their meeting controls, which exposes all of Zoom's existing in-meeting security controls in one place. This includes locking the meeting, enabling Waiting Room, and more. Users can also now enable Waiting Room in a meeting, even if the feature was not turned on before the start of the meeting. For more information, please visit this recently published [Blog](#).

Meeting ID No Longer Displayed

The meeting ID will no longer be displayed in the title bar of the Zoom meeting window. The meeting ID can be found by clicking on **Participants**, then **Invite** or by clicking on the info icon at the top left of the client window.

Setting to Allow Participants to Rename Themselves

Account admins and hosts can now disable the ability for participants to rename themselves in any meeting. This setting is available at the account, group, and user level in the Web portal.

Language for Directory and Company Directory

Domain contacts: The language in your Company directory and Directory has changed.

'Directory' is now referred to as 'Contacts', 'My Groups' has changed to 'My Contacts', and

'Company Directory' is now listed as 'All Contacts' in version 4.6.10.