Zoom policy

Getting started

- All staff taking part in zoom sessions must be appropriately trained
- Staff should run at least one trial session. This is to ensure staff know and understand protocols.
- Staff should learn how to lock a session, prevent other users from sharing their screen, place users on hold, disable and mute microphones and videos.
- All zoom sessions should be run via the Sunrise zoom account.
- Staff should use the 'schedule a meeting' icon which allows you to schedule a session in advance and set privacy and security rules for that session.
- Staff should share the hyperlink/id early to manage session.

Safeguarding

Staff should be aware of any safeguarding concerns.

Parents should be advised to monitor the session and sign their child into the session. Parents should end the session.

Staff and users should be reminded to consider what is seen in the background. Young or other children should not enter the session and no family photographs should be seen in the background.

Staff should

- Switch the settings to have microphones and videos off when joining the session
- As the host, staff should join at least 5 minutes before the session starts to manage users
- Disable 'join before host' option
- Learn how to mute and unmute all participants
- Introduce raise your hand' feature
- Use the whiteboard and annotation tools to improve engagement
- Remind users about respecting others
- Wear Sunrise uniform and name badge and talk appropriately
- Clear browser after the session
- Enabling the "Co-Host" option so you can assign others to help moderate

Important privacy and security tools

- All sessions must use a password. All participant must know and enter a password to attend your session
- Enable a waiting room: You can require all participants to wait until the host lets them in either individually or all at once. This gives the host the ability to review who's in the waiting room and only admit authorised participants.
- Only allow authenticated users a further restriction that allows only users who have been approved and authenticated in advance.
- Restrict screen sharing. Screen sharing has been used by intruders to display pornography or other inappropriate content.
- Enable participant video on or off. You can turn it on for trusted participants and turn it off for anyone who you think might be abusive.
- Don't allow participants to join before host. Set the default as off. If off, it prevents all participants from interacting until the host joins. The off default is most secure.
- Mute participants upon entry. No one can speak until you unmute them during the session.
- Lock down the session after everyone invited has arrived or 10 minutes after the session start time. This stops others joining the session.

Dealing with behavior during a session

If a person is not behaving appropriately there are a number of things the host can do. Access the in-meeting controls by clicking on participants, selecting a participant at the bottom of your screen. That brings up a list of participants. You can click on any participant's name you can then:

- Turning off people's microphones (muting)
- Ejecting them from the session
- Turn off their video
- Disable private messaging, this prevents distraction
- Disable "Allow Removed Participants to Rejoin" so ejected attendees can't re-join
- If a child/young person has been removed staff must telephone the parent as soon as possible

Evaluation

At the end of the session it is important that staff evaluates the session and makes a note of what went well and what didn't this is so that sessions can be improved.

Staff should also ask children/young people and parents to evaluate the session and incorporate this feedback into future sessions.