



Safe Zoom Learning

Our staff will make sure:

- 1) Children are invited by staff to sessions and not allowed to conduct any Zoom themselves
- 2) Staff will ensure they are not on a Zoom with a single child unless another adult is present
- 3) No other adults will be present in the video background
- 4) Staff will ensure all children leave the video call before the adults do
- 5) If there are any concerns following a Zoom that the school will follow this up with the individual/s concerned

We ask parents to make sure:

- 1) Children do not share any of their personal details with anyone in the video chat
- 2) The video conference is done with an appropriate background
- 3) An adult is available to help while getting onto Zoom, although we only require parents of Reception, Nursery and our LST groups to stay for the whole session (these are shorter)
- 4) You join the meeting at the correct time. In the event of technical difficulties, try leaving and then joining again. If this still doesn't work, please contact us via Studybugs
- 5) You talk to your child about being safe online and only talking to people that they know in real life (there is a Zoom online safety guide on the next page).
- 6) This is **not** used as an opportunity to talk with the teacher or sort any issues etc, as this will take up learning time for the other children. Please send us a message and the teacher will phone you when they are not teaching
- 7) You DO NOT use mobile phones during the Zoom session unless using the Zoom app on a phone to take part
- 8) **You DO NOT record, take screen captures, live stream during the sessions or use any recording devices to protect the GDPR of both the staff and all the children participating.**

We ask children to:

- 1) Find a quiet space to take part in your Zoom
- 2) Be kind and respectful to others
- 3) Mute when asked to by your teacher so everyone can hear
- 4) Use the chat sensibly – to ask questions or make comments about the learning, not to talk to friends about other things
- 5) Join in! Answer questions when asked and let your teacher know if you're not sure

We ask everyone to understand that we all experience technical difficulties sometimes!

As frustrating as this is, please try to stay calm and be kind. Remember if it all goes wrong that you can use the home learning information on Google Classroom or the website and your CGP books to get something done and try again the next day.



Founded in 2011, Zoom is one of the world's leading video conferencing software providers. It has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and on Android.



What parents need to know about zoom



ZOOM BOMBING

'Zoom bombing' is the term which has been coined to describe unauthorised people joining zoom meetings uninvited and broadcasting pornographic or inappropriate videos. An attacker can hijack a meeting if they know the meeting ID and it isn't reinforced with a password. Not taking preventative measures or implementing privacy controls could open up the risk of children witnessing sexual or inappropriate content with very little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in hacking operations and phishing campaigns. This is when participants are encouraged to click on links to join what they believe to be legitimate Zoom meetings via email, but which are in fact fraudulent. These scams aim to obtain sensitive information such as user login details, passwords and/or credit card information.

PRIVACY CONCERNS

Depending on how the app has been set-up, Zoom can offer very little privacy. In many cases, the meeting hosts can see detailed information about each participant including their full name, phone numbers and maybe even location data. Furthermore, depending on where the camera has been set up or where your child's computer is positioned, private or personal information could be stolen depending on what can be seen in the background.

LIVE RECORDINGS

One of the features of Zoom is the ability to record live meetings. By default, only the host of the meeting can usually record live sessions however other meeting members can also record if the host gives them access. Recordings can be stored on devices or on the cloud and can be downloaded and shared with no restrictions. This means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or between users without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a private meeting within the main Zoom session. The host can choose to split the participants of the original meeting into separate sessions. This gives children the ability to speak privately away from the main group to other users however chats aren't always monitored by the host and if the meeting has been made public, children could be more vulnerable to experiencing negative comments.

'LIVE STREAMING' RISKS

At its very core, Zoom facilitates live streaming. That means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal within a controlled environment (for instance when used in a classroom setting for remote learning). However, live streaming means that content isn't always moderated and children who use the app unsupervised or with limited security settings, may be more at risk of exposure to viewing inappropriate material. Other risks can include downloading malicious links, sharing personal information or even potential grooming.

Safety Tips For Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or upset then they need to talk about it and report it. Parents can report unwanted activity, harassment, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see something inappropriate.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and less likely to be hacked. It's important to never share meeting IDs with anybody you don't know and always set-up a password function to allow other people to sign-in. This should already be a default setting that is applied on Zoom.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number, etc. Create your child's account under a false name or pseudonym and always set a custom background to help hide details in your home. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include an unrecognisable email address, an unofficial domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chats can help to limit the risk of receiving any malicious attachments or receiving any inappropriate messages. In addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE 'VIRTUAL WAITING ROOM' FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the host to screen them before entering. This is now a default function and adds another layer of security to reduce the likelihood of zoom bombing.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix security holes and without the update you will be more vulnerable to an attack. Check the official website to see what the latest version is and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have gained everybody's permission for the session to be recorded. The host should also have set screen sharing to 'host only' and disabled 'file transfer' to help keep the live stream secure.

Meet our expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.



#WakeUpWednesday

National
Online
Safety®



SOURCES: <https://zoom.us/privacy> | <https://zoom.us/> | <https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf> | <https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing>

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 08.04.2020