Scouting at Home – Use of Video Conferencing

April 2020

Although we've had to stop our face-to-face meetings during the Coronavirus pandemic, you can still stay connected with your Section online – trying new activities, learning new skills and working towards badges and awards.

Keeping everyone safe is the number one concern for all of us at the Scouts. That's why our Adult Leaders will continue to follow the Code of Behaviour set out in the Yellow Card and encourage the safe use of the internet when working with our young people online.

There are many video conferencing platforms available and these are great tools to deliver Scouts digitally. These platforms

We will primarily be using Zoom as a video conferencing platform to deliver Scouts digitally, with our Explorers and Adults also using Microsoft Teams at times. These platforms will allow leaders, parents and young people to all be online at once so they can see and talk to one another. The Badges at Home and Programmes at Home features of Online Scout Manager will then allow us to continue making progress with activities and badges during this time.

Zoom has a minimum age of 16, so members younger than this must have their parents remain nearby throughout the meeting. Parents don't have to sit in on the meeting for the whole time, they can pop in and out. But for Beavers and Cubs, a parent should be present in the room.

Direct links for the meetings will be sent out by e-mail and available on your programme in Online Scout Manager, so there is no requirement to sign up for a Zoom account to access them. New links, meeting IDs and passwords will be generated for each session. **Do not forward them on to anyone** – if you are aware that a family hasn't received the details for a meeting, please ask them to contact their Section Leader, who make sure they can access the information.

When you click on the link to join the meeting, you will be put into the meeting waiting room. You will then be asked for your name and if you want to enable your camera and microphone. Please ensure that the member's name is used (not the parent or device name) so that the Section Leader can recognise you and then allow you to join the meeting. We use the waiting room so that our Leaders are sure who they are admitting to the meetings and that any unexpected guests are kept out.

When using live video calling, at least two Adult Leaders or Section Supporters will always be present, and both must remain on the video call until all young people have logged off. This ensures no young person is left alone with an adult online.

While participating in these sessions at home it is very important to be aware if there are other people around. Make sure those people are dressed appropriately and know how to behave while you are on the call. It might be best to ask them to stay out of the room that you're making the call from. Make sure your background space is child-friendly, ensuring nothing inappropriate is on display.

There is no requirement for your camera and/or microphone to be active during the meeting. Some members may want to fully participate, some may not but please try to encourage them to engage as much as possible. Please talk to your Section Leader or Group Scout Leader (gsl@harwellscouts.org.uk) if you or your child has any concerns about any of our online systems and their use.

Scouts

Version 7. Nov 2018
scouts.org.uk/safeguarding

This card contains essential information for all adults in Scouting. Please keep it with you at all times.

Young people first

Safeguarding – a code of practice

What do I do if...?

If a young person tells you they are being abused, you must:

1. Allow them to speak without interruption, and accept what they say
2. Be understanding and reassuring – do not give your opinion
3. Tell them you will try to help but must pass the information on
4. Tell your Group Scout Leader or District Commissioner immediately
5. Write careful notes of what was said using the actual words
6. Include the time and date and full names of those involved
7. Sign and pass your notes to your Group Scout Leader or District Commissioner
8. Make sure that Scouting poses no further risk to their welfare

If you are concerned about the welfare of a young person or there is a concern, complaint or allegation about an adult or yourself, inside or outside Scouting, you must:

1. Tell your Group Scout Leader or District Commissioner immediately
2. Write careful notes of what you witnessed, heard or were told
3. Include the time and date and full names of those involved
4. Sign and pass your notes to your Group Scout Leader or District Commissioner
5. Make sure that Scouting poses no further risk to their welfare

It is your duty to report ALL safeguarding concerns as a matter of urgency following the correct process.

If a young person is at immediate risk of significant harm call **999** and request Police. Inform your Group Scout Leader or District Commissioner once you have done this.

You must refer any concern or complaint to your GSL or DC as a matter of urgency. DO NOT investigate it yourself.

If you are in any doubt about what to do, contact the Scout Information Centre on **0345 300 1818** or **safeguarding@scouts.org.uk**
You can also contact the NSPCC on **0808 800 5000** or **help@nspcc.org.uk**

There are other organisations that you can also go to for further information and advice, such as the NSPCC. Other organisations can be found on our website.

It is the policy of the Scouts to safeguard the welfare of all young people by protecting them from neglect and from physical, sexual and emotional harm.

All members have a duty to report concerns or suspicions and a right to do so in confidence and free from harassment.

Code of behaviour

Crystal Mark 20289
Clarity approved by Plain English Campaign

Do remember that you are a role model at ALL times, inside and outside Scouting. Set a good example for others to follow.
Do treat everyone with dignity and respect in line with the Scouting Values
Do treat all young people equally - do not show favouritism
Do follow the adult-to-young person ratios at all times
Do remember that you have been placed in a position of trust - do not abuse this
Do report all allegations, suspicions and concerns immediately

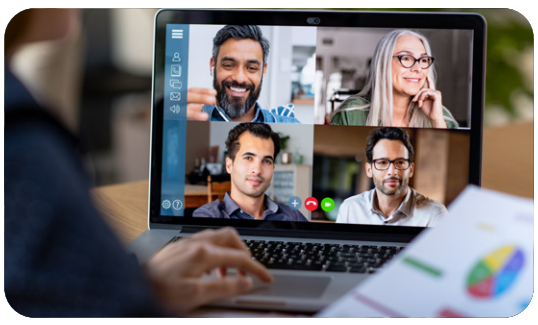
Do remember that someone may misinterpret your actions
Do respect a young person's right to personal privacy
Do act within appropriate boundaries, even in difficult circumstances
Do encourage an open and transparent culture, where people can challenge inappropriate attitudes or behaviours
Do make everyone (young people, parents and carers, Young Leaders and other helpers) aware of our safeguarding arrangements and share our Yellow Card - our Code of Behaviour
Do create an environment where young people feel safe to voice their concerns

Do have separate sleeping accommodation for young people, adults and Young Leaders working with a younger section
Do plan activities that involve more than one other person being present, or at least within sight and hearing of others. Do not plan to be alone with a young person.

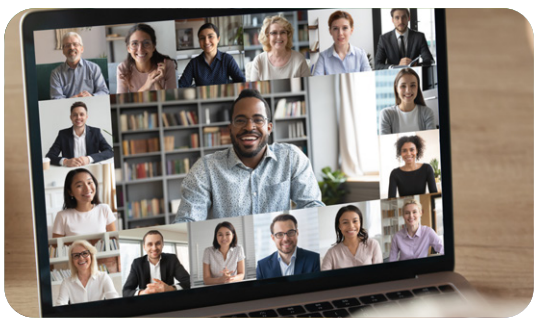
Do not drink alcohol when you are directly responsible for young people and never allow young people on Scouting activities to drink alcohol
Do not trivialise abuse or let it go unreported
Do not join in physical contact games with young people

Do not overstep the boundaries between yourself and young people by engaging in friendships or sexual relationships
Do not allow activities that encourage bullying behaviour including initiation ceremonies, dares or forfeits
Do not use inappropriate, suggestive or threatening language, whether verbal, written or online
Do not rely on your reputation or position to protect you

Founded in 2011, Zoom is one 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.

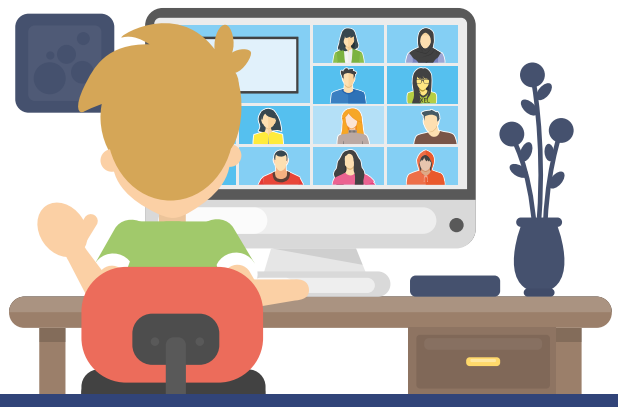
HOST IMPLEMENTED PRIVACY CONTROLS

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.

National Online Safety®
#WakeUpWednesday



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