

Online Safety

HOW TO KEEP YOUR CHILD SAFE ONLINE



EVER CHANGING

EVER EVOLVING

EVER GROWING

HOW DO YOU KNOW THAT YOUR CHILD IS SAFE?

Contact your Internet Provider



Safer Internet Day

Get Involved

Training & Events

Advice Centre

Hotline

Helpline

Pupil powered e-safety



How to set up the parental controls offered by BT



How to set up the parental controls offered by Sky





CLICK HERE for UK Safer Internet Centre

What devices are your children using?



What apps and online games are your children using?

What are their age restrictions?



It's time to get #OnlineSafetySavvy.

Children are spending more time than ever online. As adults, we need to do everything we can to keep them safe in the digital world. But with new apps, games and platforms emerging every day, how can you stay in the know?

Say hello to the new National Online Safety mobile application. Created by experts, developed by us.

With all online safety knowledge available at your fingertips, the NOS app empowers parel and

teachers to understand and address online safeguarding risks - any time, anywhere.

The world's most comprehensive online safety app, it's packed with insightful courses, explainer

videos, webinars and guides on topics that will help you protect the kids you care about when they're online.







National Online Safety

Last Viewed

69%

Download for apple: CLICK HERE

Download for android: **CLICK HERE**



Visit our school website E-Safety page - CLICK HERE



What parents need to know about

HOOKED ON SCROLLING

SLIDING INTO DMS

INFLUENCER CULTURE

IN-APP PAYMENTS

HIJACKED HASHTAGS

IGTV 💍

RESTRICT DIRECT MESSAGES

LOOK OUT FOR #ADS

MANAGE NEGATIVE INTERACTIONS

MANAGE DIGITAL WELLBEING

PROTECT PERSONAL INFORMATION

USE A PRIVATE ACCOUNT

FILTER INAPPROPRIATE COMMENTS

REMOVE PAYMENT METHODS





linesafety Facebook - /National OnlineSafety Instagram - @national onlinesafety

Meet our expert

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

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.



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' 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.



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





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.



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.

USETHE'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.









AGE LIMIT CHANGE

Since May 2018, the minimum age for using WhatsApp is 16 years old if you live in the European Union, including the UK. Prior to this, the minimum age was 13, which still applies for the rest of the world. WhatsApp has not yet stated whether it will take action against anyone aged between 13 and 16 who already hold accounts under the old terms and conditions, such as closing their account or seeking parental permission.

SCAM MESSAGES

Occasionally on WhatsApp, people receive spam messages from unauthorised third parties or from fraudsters pretending to offer prizes to 'lucky people,' encouraging recipients to click on a link to win a prize. A common scam involves messages warning recipients that their WhatsApp subscription has run out with the hope that people are duped into providing their payment details. Other scam messages include instructions to forward the message in geturn for a reward or gift from WhatsApp or another person.

FAKE NEWS AND HOAXES

WhatsApp has been linked to enabling the spread of dangerous viral rumours. In India, for example, a number of attacks appear to have been sparked by false rumours shared on WhatsApp.

THE 'ONLY ADMIN' FEATURE AND CYBERBULLYING

Cyberbullying is the act of sending threatening or taunting text messages, voice messages, pictures and videos, with the aim to hurt and humiliate the receiver. The group chat and group video call features are great for multiple people to chat simultaneously, but there is the potential for people to hurt others with their comments or jokes. The 'only admin' feature gives the admin of a group chat greater control over who can

send messages. Whilst this can be good for one-way announcements, the group admin has the power to block somebody from responding to an offensive message in a chat, which could result in a child being upset and unable to reply.

CONNECTING WITH STRANGERS

To start a chat in WhatsApp, you need to know the mobile number of the contact you want to speak to and they also need to have the app downloaded. WhatsApp can find contacts by accessing the address book of a device and recognising which of those contacts are using WhatsApp. If your child has shared their mobile number with some-body they don't know, they can use it to get in touch via WhatsApp.

LIVE LOCATION SHARING

WhatsApp's 'Live Location' feature enables users to share their current location in real time to their contacts in a chat, allowing friends to show their movements. The feature, which can be found by pressing the 'attach' button, is described by WhatsApp as a "simple and secure way to let people know where you are." Location-sharing is already a common feature on other social apps, including Snapchat's Snap Map and Facebook Messenger and can be a useful way for a child to let loved ones know they are safe. However, if your child is in a group chat with people they do not know, they will be exposing their location.



CREATE A SAFE PROFILE

Even though somebody would need your child's phone number to add them as a contact, as an extra security measure we suggest altering their profile settings to control who can see their profile photo and status. The options to choose from are 'Everyone,' 'My Contacts' and 'Nobody.' We suggest selecting 'My Contacts' or 'Nobody' to ensure their profile is protected.

EXPLAIN HOW TO BLOCK PEOPLE



If your child has received spam or offensive messages, calls or attachments from a contact, they should block them. Messages and status updates sent by a blocked contact will not show up on the phone and will stay undelivered. Blocking someone will not remove this contact from the contact list – they will need to be removed from the phone's address book. To block a contact, your child

Top Tips Parents

REPORT SCAM MESSAGES

Advise your child not to tap, share or forward any message that looks suspicious or sounds too good to be true. When your child receives a message from an unknown number for the first time, they will be given the option to report the number as spam directly inside the chat. They can also report a contact or a group as spam using the following steps: 1) Open the chat.

2)Tap on the contact or group name to open their profile information. 3) Scroll to the bottom and tap 'Report Spam.'

LEAVE A GROUP

If your child is part of a group chat that makes them feel uncomfortable or has been added to a group they don't want to be part of, use the group's settings to show them how to leave. If someone exits a group, the admin can add them back in once, If they leave again, they cannot be added again.

USING LIVE LOCATION SAFELY

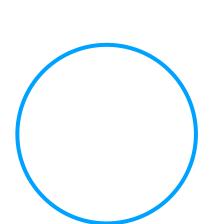
function the distribution of the distribution

DELETE ACCIDENTAL MESSAGES

If your child has sent a message to the wrong chat or if a message they sent has contained a mistake, they can delete it. To do this, simply tap and hold on the message, choose 'Delete' and then 'Delete for everyone.' The app allows seven minutes to delete the message after it has been sent, but it is important to remember that recipients may have seen and screenshot a message before it was deleted.

SET TIME LIMITS

A 2017 study found that by the age of 14 the average child will have sent more than 35,000 texts, 30,000 WhatsApp messages and racked up more than three solid weeks of video chat. Although it is inevitable that your child will use



Signs of Cyber Bullying?

It is not always easy to spot the signs of cyber-bullying. Communication devices and apps now mean that children have the opportunity for constant communication. Be alert to changes in your child's behaviour.

Being upset after using the internet or a mobile phone. Being unwilling to talk or being secretive about online activities and mobile phone use.

Spending much more or much less time texting / gaming / communicating online.

New phone numbers, texts, emails showing up on their devices.

After using devices, being withdrawn, upset or outraged. Not wanting to go to school or meet with friends.

Avoiding situations they have formerly enjoyed.

Difficulty sleeping.

Low self-esteem.

Good Habits for Parents

Taken from our 'Good Habit for Children' on the school E-Safety webpage.

- Be aware of any APPs your children are using to communicate with others on their phones.
- Keep computers and devices in open spaces in the house.
- Make yourself aware of the age restrictions of the APPs
- Talk openly with your child about their online activity and the different forms of cyber bullying. This will ensure children are aware of what is acceptable and unacceptable to say online and know they can discuss any concerns with you.
- Ensure you know how to report bullying online.
- Use parental controls to manage the content of what children are able to access online.
- Check messages to ensure you are fully aware of the content of messages being sent and received online.
- Be aware of the risks of using APPs where anyone can start a communication with your child.

Good Habits for Children

Taken from our 'Good Habit for Children' on the school E-Safety webpage.

- If you are a target of bullying it can be stopped and can usually be traced.
- Always use privacy settings
- Always respect others. If you wouldn't say it to someone's face, do not say it online.
- Be careful of what pictures you send of yourself, or someone else. Once a picture or video is sent, you can never take it back.
- Never retaliate or reply to offending emails, messages or online conversations.
- Think carefully about the things you write and how you behave online. Don't become a bully, even if you think it is a joke, if someone might be hurt or worried about it, don't send it.
- If you feel you need someone to talk to you can phone Childline 08001111

WHAT IF I HAVE A CONCERN?



Speak with your child

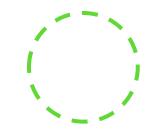
E-Safety
officer is
notified and
will
investigate

Review of policies. E-Safety committee may meet. Follow up checks with those involved.

Report the incident to school

Support and consequences considered in line with Behaviour Policy







Twitter @middparish



Email office@middletonparishce.rochdale.sch.uk



Phone 0161 643 0753

