Peterborough Diocese Education Trust

ACHIEVING MORE TOGETHER

REMOTE EDUCATION: GUIDELINES FOR PARENTS / CARERS AND PUPILS

Cranford Church of England Primary School

Original Version – May 2020
Last Updated – January 2021

Remote Education: Guidelines for Parents / Carers and Pupils

'Live' teaching delivered remotely and remote meetings (in this document referred to as 'live sessions') are a way of delivering virtual learning and conducting pastoral calls (with a child) during this COVID-19 period. The schools / academies within Peterborough Diocese Education Trust (the Trust) are providing live sessions to ensure teaching and learning can continue and calls can be made to check on pupils' welfare but, for many, this is still a new experience and **everyone involved in live sessions must remember that the usual school protocols still apply**. We are providing this guidance to ensure that participants are clear about the expectations on them.

Parents / carers:

- Parental / carer approval must be given before pupils may participate in live sessions.
- Staff at the school that the child attends will deliver live teaching. However, sometimes the school may use third party providers to deliver tutoring, interventions and / or coaching and such sessions may be live, but delivered remotely. Cranford C E Primary School use ABC Teachers for these purposes. Before any such tutoring, intervention or coaching is provided, ABC Teachers will request parental / carer consent via their standard agreement and parents / carers must ensure that they abide by the conditions in the agreement.
- Parents / carers should be aware that other staff from the Trust may occasionally be present during live sessions for monitoring purposes.
- Links for live teaching will be provided via email to parents.
- If a child is to receive a pastoral call information and video session invites will be sent directly to the parents via email.
- A parent / carer, or another appropriate adult, must be present in the room with the child for the duration of live sessions.
- Parents / carers must identify a suitable location for their child to use for live sessions, for example a living room or dining area. Bedrooms should not be used.
- Parents / carers should ensure that, as far as possible, distractions are removed, including pets and siblings, and there is quiet.
- Parents / carers should make every effort to support live sessions by ensuring their child is suitably dressed, prepared and ready to learn / engage. The expectation to wear school uniform during 'live' teaching is at the discretion of each individual school / academy.
- Parents / carers should familiarise themselves with the expectations of pupils set down in the school's guidance (based on these Trust guidelines) and ensure their child adheres to them.

- Parents / carers are responsible for ensuring that the privacy of other family members is maintained during live sessions.
- Lessons delivered 'live' are still lessons and pupils are expected to present themselves and behave appropriately. High standards of behaviour are expected for live sessions, just as they are in the classroom.
- Parents / carers should not use these live sessions as a means for communication between parents / carers and teachers. Such communication should be via email, in the first instance, in the usual way.
- Parents / carers must not record or share these live sessions, nor comment on public forums about individual teachers or other children.
- Parents / carers should be aware that the school may record lessons for:
    - future use; and / or
    - quality control; and / or
    - assessment purposes; and /or
    - safeguarding purposes.
- Parents / carers should read and familiarise themselves with the attached guidance from National Online Safety (Appendix 1) and also via: https://nationalonlinesafety.com/guides/zoom.

Pupils:

- Treat your live sessions as you would any other lesson. Be on time and be prepared.
- Use the bathroom and eat before (not during) your session.
- If it is to be a lesson, be ready to learn and make sure you have class resources, pen / pencil / ruler / exercise book at hand.
- Make sure you are in a suitable location; your device is charged (or plugged in) and that you are suitably dressed, prior to the beginning of each session. Your school / academy may have asked you to wear school uniform.
- Keep your device on a secure surface, such as a table.
- Check your camera and microphone are working, prior to the start of the session.
- If possible, you should wear a headset (ideally with a microphone) but this isn't essential.
- Remember to behave as you would in school and abide by the school's Internet Acceptable Usage Policy and the school's behaviour rules.
- Chat functions should only be used to ask questions and to answer teacher questions as directed by the teacher.
- Raise your hand, if you have a question and use hand gestures to show understanding such as thumbs up or touching your ear for audio issues.
- Do not record or take photos of your classmates or teachers during a session.
- Listen, focus on the lesson and learn.
- Avoid distractions such as electronic devices.

- Mobile phones and smart watches should not be in the room during the session.
- Respect your teacher, your fellow learners and yourself by doing your best, just as you would in class.
- Make sure you end the session as soon as your teacher indicates to do so.
- These rules are designed to help keep you safe and, if they are not followed, school sanctions will be applied and your parents / carers may be contacted.
- Remember your school / the academy is putting these sessions on for your benefit but not everyone who tries to contact you online has your interests at heart. If you have any worries or concerns about something that has happened to you online, please speak to your parents or contact us at school on 01536 330 300.

Appendix 1 – National Online Safety – Zoom

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

'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