Remote Learning Policy

Policy Creation and Review	
Author(s)	**Boleyn Trust Governing Body**
Last Review Date	**30th September 2020**
Ratified by Governing Body	**22nd September 2021**
Next Review Date	**1st September 2022**

Contents Page

1. Aims

This remote learning policy for staff aims to:

> Ensure consistency in the approach to remote learning for pupils who are not in school

> Set out expectations for all members of the school community with regards to remote learning

> Provide appropriate guidelines for data protection

In the event of a school closure, the school is committed to providing continuity of education to its learners and will do so through a process of remote (online) learning. Extensive remote learning would apply particularly in a situation in which the school is closed for an extended period, but a high proportion of learners and teachers are healthy, and able to work as normal from home or school. This policy does not normally apply in the event of short-term school closures (e.g. because of inclement weather) or a short-term learner absence.

Remote learning may also be appropriate in situations when learners, in agreement with the school, have a period of absence but are able to work at home, at least to some extent. This may apply in cases such as exclusion from school, or longer-term illness, assuming learners are able to complete school work at home. Another relevant instance would be if, following an infectious disease outbreak, learners are self-isolating at home but are not suffering with relevant symptoms.

There is no obligation for the school to provide continuity of education to learners who absent themselves from school, with or without parental permission, in contravention to school or government guidance. This may apply, for example, if parents choose to take learners on holiday during term time. Similarly, this would apply if parents made the decision, without prior agreement with the school, to absent their child/ren from school 'as a precaution', against official guidance, in the event of an outbreak of infectious disease.

2. Remote Learning

2.1 Remote learning for individual learners

Assuming an absence has been agreed with the school, and the learner in question is healthy enough to work from home, the school will provide work for learners who are unable to attend in person. If this occurs for an individual learner, the learner's teacher; Inclusion Team; or member of the Senior Leadership Team will coordinate the collation of work and communication with the parent/carer.

Though every case will have its own specifics, a rough guideline for the frequency of communication between school and parent/carer would be once per week. Work will only be provided to learners in this way if there is an agreed absence lasting more than three working days.

If a significant number of learners are absent from school, but the school remains open, the Head will decide whether the method of remote learning operated will take the form outlined here, or as outlined below.

2.2 Remote learning in the event of extended school closure

In the event of an extended school closure, the school will provide continuity of education in the following ways:

a) Regular direct instruction from teaching teachers, with the ability of learners to ask questions online (via email)

b) The setting of work that learners complete, written responses (if relevant) completed electronically

c) The assessment of specific assignments that are submitted to teachers electronically and on which feedback is provided Learners and teachers are expected to have access to the internet whilst at home; the school recognises that many families may not have home printers and will therefore not require the printing of material.

The primary digital platform the school will use to deliver continuity of education is:

> Microsoft Teams: accessed via the relevant app or desktop application. This is an online learning platform for primary learners.

> The extent to which different methods of instruction are employed is likely to be determined by the length of any school closure and the ability of both learners and teachers to participate in remote learning. The school reserves the right to vary the range of methods used to provide remote learning tasks, feedback and interaction, based on the particular circumstances of any closure and based on our experience.

2.3 Live sessions

Microsoft Teams is a platform that allows resources to be shared, teachers to provide exposition, and learners to ask questions in 'real-time'. Learners will be provided with details, and will be expected to participate in them if they are asked and able to. Live sessions can be particularly helpful as they can help communication, with learners able to respond to teachers' questions (and ask them) via the conversation functionality in teams and meet.

Learners will be provided with a school email address to avoid any issues regarding GDPR, there will be no expectation for parents/carers or learners to provide their own email addresses for use.

3. Roles and responsibilities

3.1 Teachers

When providing remote learning, teachers must be available between 9am and 4pm

If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.

Unless it is specified from government guidelines, teachers will provide lessons in school or remotely at school through live streaming. When providing remote learning from home, teachers should ensure they have effective internet and phone connectivity at home. If this is not available for any reason, teachers can request a school device.

The staff code of conduct still applies when teaching remotely from home and all staff should ensure that they adhere to the dress code. They should also ensure that they are in their living room, study or kitchen etc, with nothing inappropriate in the background.

The setting and assessment of remote learning tasks will take place in accordance with school and subject area policies. Under normal circumstances, subject areas take different approaches to the setting and assessment of learners' work – for example, the frequency of substantive task set, and the regularity of written assessment provided – and subject area policies will be applied in the event of remote learning.

In order that we are providing a consistent approach, subject leaders are responsible for overseeing the nature and frequency of tasks set and assessed within their subject areas. All teachers should pay due care to the nature of tasks set, so that learners have a range of activities to complete at home and are not exclusively working on a screen. Teachers are responsible for providing constructive feedback to their learners in a timely manner.

In the event a teacher is unwell during a period of remote learning, it becomes the responsibility of the year partner teacher and their AHT to ensure work is set to her/his classes. Teachers should be available to contact parents if needed, by

ParentMail, Microsoft Teams or phone (when phoning from personal devices, dialling 141 before the number will ensure the teacher's own number is kept anonymous). If contact is deemed excessive the line manager will be able to support and, if necessary, escalate to SLT. Where possible, the school will remain open for teachers to use school phones to call children's homes. Teachers should contact a member of SLT if they are unable to access a phone for this purpose.

If parents ask for additional work beyond that set as part of the requirements above, subject areas should have a bank of general resources available and point pupils and parents in that direction.

In order to ensure teachers are able to perform the minimum expectations outlined above; the school will provide a range of training opportunities that teachers should access to before any planned school closure. Teachers should ensure that they have looked through specific instructions, watched walkthroughs, and attended teacher training sessions. If teachers require support with any aspects of remote learning, they are encouraged to consult their line managers or the Senior Leadership team.

Unless there are extenuating circumstances, teachers will be expected to be contactable remotely by colleagues, learners and parents. Teachers also should ensure their communication with learners does not encourage unhelpful work habits. All communication should take place during usual office hours, with no expectation for colleagues to read or respond to emails after 4.30pm, although responses should be made to electronic messages within one working day in normal practice. For those who are on part-time contracts, communication is expected only on the days on which they would usually work.

Communication must always occur via official school channels, and not through personal accounts or other websites. Permitted methods are:

• ParentMail
• Microsoft Teams

3.1ii   Support for pupils with SEND, EAL and other specific learning enhancement needs

Teachers should ensure that work is differentiated as required for all learners when setting online tasks. Profiles are available for SEND pupils and advice can be sought from the Inclusion Team. In addition, the Inclusion Team will maintain contact with pupils on their lists requiring regular support, by email or phone with parents/learners and feed back to teachers using the appropriate channels if required.

3.1 iii   Assessment

Providing timely and helpful feedback is a cornerstone of good teaching and learning, and whilst this may be more challenging with remote learning, teachers should endeavour to provide regular feedback to learners on pieces of work that they are required to submit. Under normal circumstances, not all pieces of work are formally assessed by teachers and this would continue to be the case should the school employ remote learning.

Given the nature of the tasks, the type of feedback teachers can provide may not have the same format as marking an exercise book. Teachers are encouraged to ensure, when they set assessed work, that it is designed in such a way that meaningful feedback may be provided.

Possible methods may include:

• Providing whole class feedback rather than feedback on individual pieces of work – this is an effective way of providing feedback, supported by findings from educational research
• Using the "Comments" function on online documents or Microsoft Teams
• Sending a direct to learners with specific feedback / targets
• Feedback via another website / piece of software

3.1 iv   Pastoral care during a school closure

In event of a school closure, the primary responsibility for the pastoral care of a learner rests with their parents / carers. However, teachers (under the guidance of the Senior Leadership Team) should check in regularly to monitor both academic progress and their general wellbeing. Teachers will be expected to pass on feedback to the Inclusion Team & Senior Leadership Team, particularly if there are concerns or a lack of communication.

3.1 v   Safeguarding during a school closure

In the event of a school closure, pupils, parents, carers and teachers are reminded that the school's Child Protection and Safeguarding Policy still applies to all interactions between pupils and teachers. In that policy, there are specifically prohibited behaviours and reporting obligations to which teachers must adhere, whether they are at home, in the community or at school.

3.1 vi   Behaviour Support Service Support during a school closure

In the event of a school closure, the Safeguarding Team may maintain support or interventions with children and young people through Teams. Staff are reminded that the home school's Child Protection and Safeguarding Policy still applies to all interactions between pupils and staff. The BSS team could also attend multi-agency or SEND meetings during this time.

3.2 Teaching assistants

When assisting with remote learning, teaching assistants must be available between 9am and 3:30pm

Unless it is specified from government guidelines, teachers will provide support in school or remotely at school through live streaming and using breakout rooms for interventions. If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.

When assisting with remote learning, teaching assistants are responsible for:

> Supporting pupils who aren't in school with learning remotely i.e working with focused group or providing their intervention sessions through Microsoft Teams and or Zoom.

Attending virtual meetings with teachers, parents and pupils –   Therefore the staff code of conduct still applies when teaching remotely from home and all staff should ensure that they adhere to the dress code. They should also ensure that they are in their living room, study or kitchen etc, with nothing inappropriate in the background.

3.3 Subject leads

Alongside their teaching responsibilities, subject leads are responsible for:

> Identifying if any aspects of the subject curriculum need to change to accommodate remote learning

> Working with teachers teaching their subject remotely to make sure all work set is appropriate and consistent

> Working with other subject leads and senior leaders to make sure work set remotely across all subjects is appropriate and consistent, and deadlines are being set an appropriate distance away from each other

> Monitoring the remote work set by teachers in their subject through regular meetings with teachers or by reviewing work set

> Alerting teachers to resources they can use to teach their subject remotely

3.4 Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

Insert details, such as:

> Co-ordinating the remote learning approach across the school

> Monitoring the effectiveness of remote learning through weekly phase meetings with teachers and regular meeting subject leaders, reviewing work set or reaching out for feedback from pupils and parents

> Monitoring the security of remote learning systems, including data protection and safeguarding considerations

3.5 Designated Safeguarding lead

The DSL is responsible for:

> The Designated Safeguarding Lead (DSL) in school takes the lead responsibility for managing child protection referrals, safeguarding training and raising awareness of all child protection policies and procedures in school and that everyone in school, including temporary staff, volunteers and contractors are aware of these procedures and that they are followed at all times.

> They are a source of advice and support to other staff on child protection matters and make sure that timely referrals to Newham Triage Team are made in accordance with current London Child Protection Procedures. The Designated Safeguarding Lead (DSL) works with the local authority and other agencies as required. If for any reason the Designated Safeguarding Lead is unavailable, the Deputy Designated Safeguarding Lead will act in their absence.

> In addition, in most cases homelessness would be considered in the context of children living with their families, however the Designated Safeguarding Lead (DSL) will be alert that some children may be homeless independently and this will require a different level of intervention and support.

3.6 ICT Resource Manager

ICT Resource Manager is responsible for:

> Fixing issues with systems used to set and collect work.

> Helping staff and parents with any technical issues they're experiencing

> Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection officer

> Assisting pupils and parents with accessing the internet or devices

3.7 Pupils and parents

Staff can expect pupils learning remotely to:

> Be contactable during the school day although they may not always be in front of a device the entire time

> Attend relevant live sessions.

> Complete work to the deadline set by teachers to the best of their ability

> Seek help if they need it, from teachers or teaching assistants

> Alert teachers if they're not able to complete work

> Read and respond to communication from the school through Microsoft Teams on a regular basis.

Staff can expect parents with children learning remotely to:

> Make the school aware if their child is sick or otherwise can't complete work

> Seek help from the school if they need it – if you know of any resources staff should point parents towards if they're struggling, include those here

> Be respectful when making any complaints or concerns known to staff

3.8 Governing board

The governing board is responsible for:

> Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible

> Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

4. Who to contact

If staff have any questions or concerns about remote learning, they should contact the following individuals:

> Issues in setting work – talk to the relevant subject lead or Inclusion Team
> Issues with behaviour – talk to the relevant Phase Leader/AHT
> Issues with IT – talk to IT Resource Manager
> Issues with their own workload or wellbeing – talk to their line manager
> Concerns about data protection – talk to the data protection officer
> Concerns about safeguarding – talk to the DSL

5. Data protection

5.1 Accessing personal data

When accessing personal data for remote learning purposes, all staff members will:

> Ensure that they access the data, if permitted, within the usual channels at school such as on a secure cloud service (ParentMail) or on SIMs.
> Staff should ensure that they use the devices provided to access the data, such as laptops, rather than their own personal devices.

5.2 Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

> Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
> Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
> Making sure the device locks if left inactive for a period of time
> Not sharing the device among family or friends
> Installing antivirus and anti-spyware software
> Keeping operating systems up to date – always install the latest updates

6. Safeguarding

Staff can find and access our safeguarding policies and procedures both on the school website as well as within our online 'Staff Handbook'.

7. Monitoring arrangements

This policy will be reviewed annually by SLT unless government guidelines change, then it may be more frequent. At every review, it will be approved by the Boleyn Trust.

8. Links with other policies

This policy is linked to our:

> Behaviour policy
> Child protection policy
> Data protection policy and privacy notices
> Home-school agreement
> ICT and internet acceptable use policy
> Online safety polic

Appendix 1 – Remote Learning Agreement

1. I will only use ICT systems in school/home, including the internet, e-mail, digital video, mobile technologies, for school purposes.

2. I will only use my school e-mail address for school related things.

3. I will not attempt to bypass any computer or user account restrictions to access confidential or otherwise restricted information on the school network.

4. I will not try to bypass the internet filtering system.

5. I will make sure that all electronic communications with pupils, teachers or others are responsible and sensible.

6. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

7. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.

8. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.

9. I will follow the school approach to online safety and not deliberately record/video upload or add any images, video, sounds or text that could upset or offend any member of the school community

10. I will respect the privacy and ownership of others' work on-line at all times.

11. I understand that all my use of the Internet and other related technologies will be filtered, and can be monitored, logged and made available to teachers, to protect me and others and the integrity of school systems.

12. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer will be contacted.

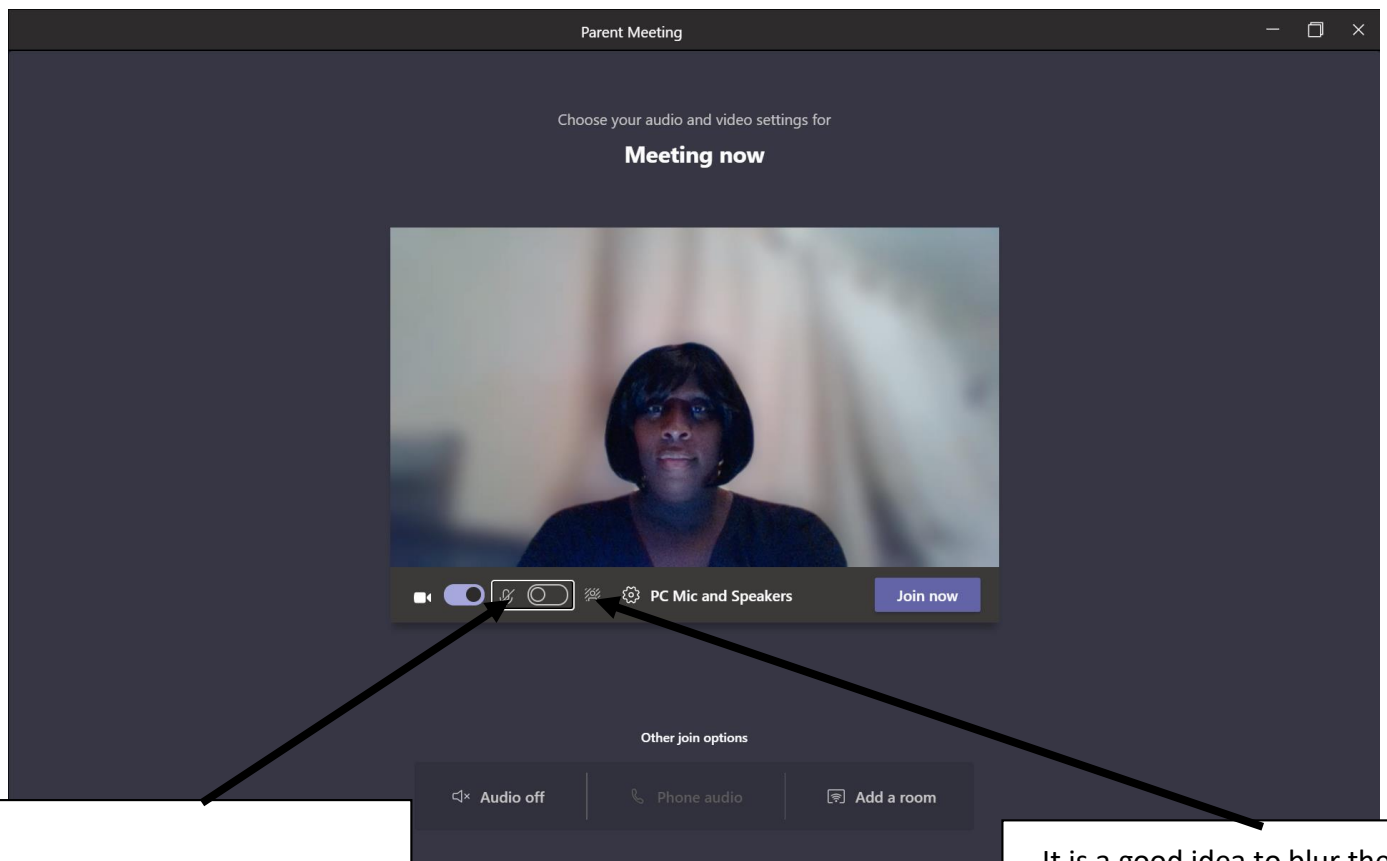| Student Name:	
Signed Pupil	
Signed Parent/Carer	
Signed Staff member:	

Appendix 2

Videoconference Lessons

During video calls with your teachers it is really important that you stick to these rules:

1. An adult is with you during the video call
2. You are in either your dining room, living room or kitchen and not your bedroom.
3. You must be dressed and ready – not in pyjamas.
4. Please remember that the video conference is part of school. You must be respectful to staff and other pupils. School rules still apply!
5. Staying safe online – keeping yourself, your classmates and your teacher safe.
6. Do not record or take pictures of your teacher or classmates during you online sessions.

Joining the video call

> Your teacher will send you an invitation to join a meeting on Teams. Which will come through in an email.

> Open the invitation and click on yes.

> Go onto the calendar, you should be able to see the meeting on the calendar.

> Click on Join.

You will have the option to join in the app or to join using the browser. If you can download the Teams app it works better.

Parent Meeting

Choose your audio and video settings for
Meeting now

PC Mic and Speakers

Join now

Other join options

Audio off   Phone audio   Add a room

Start with your microphone muted (turned off) otherwise it gets very noisy.

It is a good idea to blur the background so everyone in your class can't see all of your house.

Microsoft Teams, or simply 'Teams', is a platform that allows for collaborative working, either as students or as professionals, using communication capabilities through audio, video and instant messaging. The software is available both online through a web browser and to download from microsoft.com. Users can have 1:1 online meetings or set up live events to host up to 10,000 people. Groups can be set up to include only relevant users and almost all file-types can be uploaded and shared, from PDFs and Word documents to audio and video files.

AGE RESTRICTION 13+

What parents need to know about
MICROSOFT TEAMS

DISCLOSING PERSONAL DETAILS

Like any messaging service or social network, children can be targeted by others to share their private or personal information ranging from their phone number, birthday and home address to their social media accounts or even their personal login details and passwords. Oversharing their private information can lead to any manner of risks including online fraud, bullying or even grooming activity.

CYBERBULLYING

The risk of cyberbullying can be increased online when using chat facilities. Microsoft Teams provides the ability for users to chat to each other via its instant messaging service, both as part of a group or privately. Children could find themselves the target of negative or hurtful comments directed from other users who might find it easier to say things they maybe otherwise wouldn't in person.

INAPPROPRIATE CHAT

The chance to have private conversations in Teams can also mean that children feel as though they can share messages and communication between each other that are hidden away from others. Whilst children are most likely to use Teams in a school setting, the ability to chat privately may provide an opportunity to be less formal which could lead to sharing inappropriate messages, files or content which is unsuitable in a school environment.

HACKING RISK

Teams, like any software application, may be a target for hackers to illicit personal data. A 'man-in-the-middle attack' could occur, whereby the attacker reroutes communication between two users through the attacker's computer without the knowledge of the other users. This means that online communications could possibly be intercepted and be read or listened to, exposing both parties to the possibility of identity fraud or other criminal behaviour.

VIRUS INFECTION

Viruses and other harmful programs are among the risks of using online platforms like Microsoft Teams. Wherever you can share files or links, there is a risk that the content could be malicious. This could lead to slow computer performance, deletion of data, the theft of private or personal information and even hackers taking control of your PC.

LIVE STREAMING RISKS

Microsoft Teams, like other video-conferencing software platforms, facilitates live streaming. That means it inevitably carries some of the associated risks. These are likely to be minimal within a controlled environment (for instance in a classroom setting / remote learning). However, live streaming means that content isn't always moderated and children may inadvertently view or hear inappropriate, unsuitable or offensive material that they otherwise wouldn't.

NOS National Online Safety®
#WakeUpWednesday

Safety Tips for Parents & Carers

BLOCK USERS

If your child is receiving inappropriate messages or finds themselves being harassed or abused on Teams, they can block these contacts from the privacy control in the settings menu. To add an extra layer of protection, you can also block contacts whom hide their ID to protect children from communicating with people they don't know.

PROTECT PERSONAL INFO

It's a good idea to talk to your child about the importance of keeping their personal information private and secure. Children should only give out the minimum information they need to when creating an account and understand that if other people request their personal details from them, they should avoid providing it and report any concerns to a trusted adult.

ENABLE BACKGROUND BLUR

To help protect your privacy during a video call or live stream, it may be a good idea to blur the background or even add a background effect. This can easily be done by clicking 'Background effects' before joining a meeting after which you'll have the option to blur your background, replace your background with one of the images provided or upload and use an image of your own.

UPDATE COMPUTER SECURITY

It's important to ensure you perform regular computer and software updates, as these patches often improve security flaws and minimise your vulnerability to cyberattacks. Having your own computer security or anti-malware software is another level of defence in minimising the chances of an attack from viruses, malware and other harmful programs. Ensure this is updated everyday so that it is able to protect you against the very latest threats.

TALK ABOUT RISKS

As a parent, talking to your child and making them aware of the risks of working and communicating online can help them to be more digitally resilient. Perhaps outline a set of agreed do's and don'ts and try to ensure young people know what to do if they are made to feel uncomfortable or experience any negative behaviour or activity.

AVOID VIDEO/AUDIO

It's always a good idea to turn off your audio during live group calls when not in use. This can easily be done by muting the mic and will avoid others hearing anything personal in the background at home or at school. Similarly, if possible, try to encourage children to avoid using video call to help guard against any privacy concerns and limit the risks of viewing anything inappropriate or unsettling.

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.

SOURCES:
https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/group-chat-software
https://www.microsoft.com
https://www.thinkuknow.co.uk

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 ensure 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.

NOS National Online Safety®

#WakeUpWednesday

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

10 TOP TIPS
REMOTE LEARNING FOR TEACHERS

Remote learning can be a great way to continue learning outside the classroom, particularly in difficult circumstances. For school staff and teachers, there is a lot to consider and planning is key to ensuring a smooth transition from classroom to home. That's why we've created these top tips to help school staff ensure they deliver the most secure and safest remote learning experience they can, both for themselves and their students.

1) Familiarise yourself with the relevant policies

Whilst remote learning might be unchartered territory for you and your school, ensure you still adhere with the relevant policies around safeguarding, acceptable use, data protection, student behaviour and online conduct, for example.

2) Consider your surroundings

The use of webcams, video and live streaming must be done with careful thought. Ensure the positioning of any camera is in an open space with a plain background if possible and with no personal information on display. Avoid bedrooms.

3) Create and disseminate a clear distance learning policy and guidance

This is important so that parents and pupils are clear as to what is expected of you, including around behaviour and conduct. It will also provide them with a level of confidence and reassurance.

4) Only use school approved platforms and communication channels

Make sure that you keep to communicating through official outlets, such as your school online portals or assigned email addresses. Never communicate using personal emails or numbers and refrain from communicating outside of school hours.
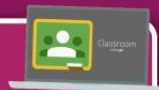
5) Maintain professional dress at all times

Treat any online lesson the same as delivering a lesson in the classroom. Maintain a professional image and never wear anything inappropriate or revealing. Encourage your students to also wear their school uniform.

6) Distribute a class timetable/schedule for remote learning

This will help to maintain a structure and lesson plan to classes. Include the frequency of lessons, duration, how they will be delivered, times for online and offline learning and any links. This will give parents a sense of structure and reassurance around lesson delivery.

7) Ensure you use the correct/ appropriate technology

Remote learning will mean that you will need to employ the right technology and software to ensure that students are able to access learning in the safest and most secure way. Look to distribute a list of safe apps and software that are secure and won't raise any safeguarding concerns.

8) Protect personal data

Only use appropriate systems and software that require email and password login. It's always best-practice to only use school-provided email addresses.

9) Consider the needs of SEND pupils and vulnerable learners

It's important to try and accommodate all students, including children with SEND or those who are more vulnerable, and take into account different levels of learning.

10) Try to make lessons fun and engaging and encourage regular feedback

Remote learning is a fantastic way to be imaginative with teaching and learning and a great way to encourage independent thinking. Try to encourage a two-way flow of communication with parents and students to help maintain transparency and confidence in the learning process.

National Online Safety®
#WakeUpWednesday

10 TOP TIPS
REMOTE LEARNING FOR CHILDREN

Remote learning can be a great way to continue learning outside the classroom, particularly in difficult circumstances. For students, it's the perfect way to ensure they still get the education they need, despite not being at school. However it also requires a level of discipline and careful planning. That's why we've created this guide to help pupils understand different aspects of remote learning and to support them in ensuring their experience is as safe and secure as it can be.

1) Treat remote learning the same as classroom learning

Despite being at home, it's important to remember the same rules apply as being in the classroom, particularly in respect of behavior and conduct. Focus on learning and don't get distracted by your surroundings.

2) Use classroom language

If you are encouraged to communicate through emails and online messages, don't use shorthand text speak and write as though you would speak in class. Remember to be respectful and polite and avoid positing negative comments or spamming the chat.

3) Take regular screen breaks

Whilst remote learning might be an exciting experience to begin with, having prolonged periods of time in front of a screen isn't always healthy. Remember to have regular screen breaks where possible and in your spare time, try to get some fresh air and enjoy other activities away from electronic devices.

4) Always conduct video learning in an open space at home

To get the best experience from remote learning, it's important to create the right environment around you. Try to set up a mock 'classroom desk' at home in an open space so parents can supervise if necessary. Avoid bedrooms as this could be considered inappropriate.

5) Only communicate through approved school portals and platforms

It's important that you send messages and any pictures or images required for class through approved school channels, such as internal learning portals or approved platforms. This will help to keep your personal information safe and secure.

6) Stick to teacher rules and guidelines around online learning

Your school should issue you with guidance around remote learning and the rules to follow. Always maintain classroom behaviour and try to remember that you are in a learning environment and not a social setting.

7) Dress in school uniform

As part of your learning environment, try to maintain school uniform/dress. This will help as part of replicating classroom learning in the home. Try to avoid wearing anything too casual as this could be deemed inappropriate for school.

8) Don't share passwords or other sensitive information

In order begin your online lessons or to gain access to learning materials, you may be provided with login details and passwords. In the same way you keep your personal details private, always keep these safe and never share them with others.

9) Don't use school platforms to discuss personal matters

It's important to keep your school communication channels separate from your own personal communication with friends and family. Don't be tempted to engage in casual discussions or send images, videos or links via official school apps or platforms that aren't associated with your learning.
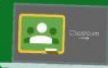
10) Look after your mental health and wellbeing

Remote learning ultimately means working alone and missing out on daily social interaction with your friends. If you ever feel frustrated, low or sad, it's important to discuss how you feel with your parents or your teacher. Keeping in touch with friends over the phone or on social media can also help to keep your spirits up.

National Online Safety®
#WakeUpWednesday

10 TOP TIPS
REMOTE LEARNING FOR PARENTS

Remote learning can be a great way to continue learning outside the classroom, particularly in difficult circumstances. For parents and carers, the idea of remote learning isn't always straightforward and there can be a number of factors they need to consider, especially around ensuring their children feel comfortable and are familiar with the whole concept. That's why we've created this guide to help parents and carers support their child in getting the most out of their remote learning experience.

1) Take an active interest in your child's learning

As a parent or carer, remote learning will be a new concept for your child and there are bound to be a few teething problems to start with. Take an active interest in their learning and help support them whenever they need a helping hand.

2) Monitor your child's communication and online activity

It's important to remind your child that despite being at home, the same level of behaviour and conduct exists as if they were at school. Encourage them to remain polite, remember their manners and not to post or send any negative comments just because they are behind a computer.

3) Establish a daily schedule and routine

Working from home and trying to learn in a more casual setting that children might associate more with play and a degree of freedom might take a bit of getting used to. Try to stick to a daily routine and use the timetable/schedule that schools have sent home to help children keep on top of their daily learning.

4) Encourage screen breaks away from devices

Remote learning will inevitably require more interaction with computers, laptops and tablets. Teacher's will invariably advise on screen breaks however it doesn't hurt to keep a check on their time online or encourage them to get some fresh air/exercise.

5) Ensure your learning device is in a public space in the home

It's important to consider where your PC or laptop is placed if live video is being used. Try to keep the background neutral with no personal information visible and move learning devices out of the bedroom as this could be deemed inappropriate.

6) Implement safety controls and privacy restrictions on apps and software

Dependant on how your school implements remote learning, your child may be required to download certain software or apps. Whilst these are likely to be relatively safe to use, like any other new app or platform, parents should still implement safety controls as a precaution.

7) Ensure your child only uses official school communication channels

It's important that all communication with teachers and school staff is directed through approved school channels, whether that be through the school's online portal or the relevant secure messaging site.

8) Familiarise yourself with relevant school policies

Schools should have a policy on remote learning and direction that they can share with parents. Familiarise yourself with this and ensure you know what is expected of teachers and your child during lessons, both online and offline.

9) Maintain feedback with teachers

Engage in communication with teachers where possible and try to feed back progress and development as well as any helpful suggestions around the learning process. Be transparent but remain professional and only use official channels to communicate.

10) Monitor your child's wellbeing and mental health

Remote learning will likely mean that your child won't get the same level of social interaction and might not see their friends for a while. Keep a check on their wellbeing and try to encourage them to get out as much as you can. Whilst learning from home might seem fun and exciting to start with, missing out on seeing their friends everyday might take its toll.

A GUIDE TO SAFER LIVE LESSONS

An online lesson occurs when teachers use video conferencing software to 'live stream' lessons to their pupils. Some of the most popular apps and websites that support this include Zoom, Google Hangouts, Skype and Microsoft Teams. Online lessons can be a great way to replicate classroom interaction, ask immediate questions and gather instant feedback. It's also convenient and allows learning to take place anywhere with an internet connection. However, live lessons aren't always accessible to everyone and younger children will need a lot of parental supervision, which isn't always practical.

What teachers need to consider

CONDUCT

If you decide to host an online lesson, it's important that you maintain a level of professionalism and treat any online lesson in the same way you would treat a classroom lesson. Dress appropriately and find a setting which has a plain background and has no personal information on display. Remind pupils of acceptable behaviour and their conduct during class. It's worth remembering that live streaming means screenshots and video recordings of your lesson could occur so you should always observe professional conduct at all times.

COMMUNICATION

Hosting a live lesson means that you will have to think about how you communicate and through what channels. Children will need access to the internet, have the appropriate technology and will need to download the relevant software or application. Some, or all, of these may not be widely available to everyone. It's also important to consider that the software that you choose to use is secure and has the relevant privacy and security settings in place. Any contact should only be through a platform provided by the school and not through personalised accounts open to public viewing, comments or sharing.

CONTENT

Planning your content will be a key factor to consider prior to hosting an online lesson. It's important to ensure that all content is age-appropriate and that any tasks that you set which require use of the internet won't lead children towards anything offensive or inappropriate. Always try to ensure that live lessons take place with the whole class but bear in mind that some pupils may work slower than others depending on the type of tasks you set.

What parents need to consider

CONDUCT

It's important to remind your child that despite being at home, the same level of behaviour and conduct exists as if they were at school. Encourage them to remain polite and remember their manners. Position your computer or webcam in an open environment where you can monitor their activity, preferably not in a bedroom. Try to keep the background neutral with good quality lighting and sound.

COMMUNICATION

If your child is part of an online lesson, they may need support in setting up the relevant software and communication platforms in order to take part. Your school will usually provide the relevant details on how to do this however it's worth ensuring that you have some awareness of the privacy and security settings so that you know that all communication is secure. It's important to raise any concerns that you have with the school if you are unable to accommodate an online lesson for any reason.

CONTENT

Try to take an interest in your child's live lesson if you can and stay close so that you can aid them if necessary. Try to find out who is hosting the lesson, what the lesson is about and what tasks they will be set. If they are required to conduct internet searches, ensure parental controls are in place. If you're using Zoom, make sure that screen sharing is only shared with the host. This will avoid 'Zoombombing' whereby uninvited guests use the screen-sharing feature to broadcast porn or other inappropriate content.

NOS
National Online Safety®
#WakeUpWednesday

SOURCES:
https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis
https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking
https://hangouts.google.com/
https://support.skype.com/en/faq/fa34649/protecting-your-online-safety-security-and-privacy
https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview

Some commonly used platforms

zoom

Zoom is one of the most popular video conferencing apps at the moment. Schools using Zoom can monitor attendee's activity while screen-sharing, track real-time activity, record live lessons and recall video, audio, transcript and chat files. Admins can also see the IP address and admin information of all attendees.

⚠ Safety Tips ⚠

✅ Change privacy controls so that screen sharing is limited to the host only.
✅ Turn file transfers off to reduce any risk of hacking or installing a virus/malware.
✅ Create a strong password for your account incorporating letters, numbers and symbols.
✅ Keep the software as up to date as possible with the latest security patches.

Google Hangouts

Google Hangouts allows communication through video, audio or messaging, although isn't end-to-end encrypted. During the COVID-19 outbreak, Google has been making the advanced features in Hangouts Meet available to all schools around the globe using G Suite for Education.

⚠ Safety Tips ⚠

✅ Ensure that any call made via the app is private or by invite only.
✅ Customise who you can receive invites from through the privacy settings to block unwanted contact.
✅ Keep all anti-virus software up-to-date and instate a firewall.
✅ Always sign out after use to prevent anyone else from accessing your account.

Skype

Microsoft owned Skype is a well-known communication tool that specialises in providing video chat and voice calls. It is one of the biggest apps in the world, providing end-to-end encryption between Skype users, as well as facilitating screen sharing and the ability to record calls.

⚠ Safety Tips ⚠

✅ Ensure you have the latest anti-virus software installed on your computer and set up a personal firewall.
✅ Keep profiles hidden and don't share any unnecessary personal information on your profile.
✅ Don't download anything from profiles you don't know and block any suspicious contacts.
✅ Always adjust privacy settings, including only allowing children to communicate with approved contacts.

Microsoft Teams

Microsoft Teams describes itself as a 'group chat software and collaboration tool'. Its provides the ability to chat, meet, call and collaborate from anywhere and is popular given it's ability to seamlessly integrate with other Microsoft applications like Word and Excel.

⚠ Safety Tips ⚠

✅ Turn off guest access so only school issued email addresses communicate.
✅ If linked to an Office 365, enable Advanced Threat Protection (ATP) to help prevent against threats via emails, links, and attachments.
✅ Make sure your operating system has the latest updates and security patches.
✅ Beware of phishing emails asking for your password – Microsoft will never ask you it.