The Aspire Educational Trust Guidance for Safety in Remote Online Video and Telephone Communication with Pupils and Parents

Contents

Introduction

Remote recorded video lessons allow teachers to deliver content to children. These can be delivered live or these can be pre-recorded, or recorded during the live session and watched later by a pupil who has missed a session or to allow the time of learning to be more flexible. These can take place on a one-to-one basis or in a class scenario where each child accesses the lesson via a secure video link.

These can be developed further to include **live teacher-student interactions** – to allow teachers to maintain face to face interactions with students in remote lessons via webcam. There is also scope in some of the software for a class 'chat' during the session, screen sharing and live annotations to ensure teachers can build a collaborative environment.

In all elements of our work online in schools, the safety of pupils, staff and our wider community is paramount and must be considered carefully. It is with this in mind, in a rapidly changing educational landscape, that this guidance is being developed by the Trust.

What is the expectation on schools to deliver online learning via video?

In England, the Department for Education (DfE) has no expectation that teachers should livestream or pre-record lessons. Schools should consider the approaches that best suit the needs of their pupils and staff (DfE, 2020). If you do plan to record or livestream lessons via an online platform, you need to assess any risks and take appropriate actions to minimise harm. This guidance is designed to support you in that.

Considerations for your school when embarking on use of video as a vehicle for communication with families and learning

Expectation - There is no expectation from Department of Education or Trust for schools to use video technology – it is a school based decision.

Research - consider what the latest research is saying about the impact of the activities you are considering to support your decision making – see EEF website

Safety of staff and pupils - Should you wish to use video technology this guidance has been designed to support you in keeping staff and pupils safe

Technology - What technology and Internet connection speed will be required for everyone to participate (e.g. devices). It is important to consider that not all students will have access to technologies that will enable them to participate in online classes. What solutions can you provide to enable them to continue learning? Loan device? Posted assignments? Phone calls with staff?

Consider activities carefully when planning – online access within school will have internet content filtering systems in place that are unlikely to be replicated in the home environment.

If you are running live sessions, how will you respond to technical glitches that can distract from the smooth running of a call?

Charges for families and staff - Be careful that staff and children don't incur surprising costs, e.g. mobile data access charges - (video utilises significant amounts of data).

Devices - We would strongly recommend that staff avoid using personal devices and should only use school provided equipment

What online platforms can I use?

Staff should communicate with parents or pupils using Trust approved channels. It is not appropriate to talk to parents or children using their personal Facebook accounts, using personal email addresses or phone numbers. Similarly, it is important to set up school accounts for any online platforms you use (not to use teachers' personal accounts).

There are some safety concerns around the use of other platforms such as YouTube or Facebook Live, even when used with restricted settings for sharing, and these should ideally not be used. For example, although YouTube can be set to a restricted audience, the video will end recommending other similar content to a viewer that will not have been approved by school and may not be suitable. In addition, although the link has been sent to a restricted audience, it can be copied and sent to a wider audience, thus removing the security.

The Trust approved platforms include Microsoft Stream, Vimeo, Microsoft Teams, Cisco WebEx Meetings and Google Meet. These can all be used, <u>following guidance for safety</u>, to both record lessons for sharing at a later date and for live lessons. Should you wish to use other platforms, please discuss with the Trust Safeguarding lead before proceeding.

At the end of this guidance document are some 'How to…' guides to support staff in use of Google Drives (including the features of G Suite for Education (e.g. Google Classroom and Google Meet)) and for Office 365 Education (including Microsoft Teams).

When considering recording videos to share, Microsoft suite now include a product called Microsoft Stream which locks down permissions for sharing. In addition, there is a product called Vimeo which is simple to use and has additional security that does ensure your videos have more secure privacy. Vimeo has a cost of £6 per month.

Please see following link for advice from a Safeguarding Consultant that helps to explain the safety features we need to be looking for in a product. https://vimeo.com/411516917 (and why You Tube is unsuitable)

With this guidance for support it is vital that a designated member of staff within school risk assesses the technology used for all remote learning, including pastoral support prior to use, ensuring that there are no privacy or safeguarding issues or scope for inappropriate use. Staff must have completed basic online safety training (available from the Trust) as well as receiving specific product feature training to ensure they understand the product features that will maximise security.

The school should ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

Consent

Before undertaking any form of video conferencing, make sure parents, carers and children understand the benefits and risks of online lessons and get written consent for children to be involved. Always use parent's or carer' email addresses for any invitations to online learning, ensuring their consent for the activity. School should also communicate with parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure and the steps the school is taking to keep their child safe online. See Annex A of this guidance for a model consent form.

Setting up your Security for Online learning

Different platforms offer different security measures that should be considered when you schedule a session: -

- **Use parent's or carer' email addresses** for any invitations to online learning, ensuring their consent for the activity.

- **Password Protect** access to the meeting/ lesson and share with your students in a **separate email** to the lesson invitation so only those intended to join can access a virtual classroom.

- **Locking your meeting**/ virtual classroom/ lesson

- **Controlling screen sharing** so this can only be done by the host or at the invitation of the host

- **Enabling a waiting room** – so the participant joins into a waiting room and waits for the host to add them to meeting individually or all at once

- **Lock down or removing the chat** – to restrict in class chat or to not allow private messaging etc. within the chat

- **Remove a participant**

- **Disable join before host:** Students cannot join class before the teacher joins and will see a pop-up that says, "The meeting is waiting for the host to join."

- **Disable the video or mute**/ unmute students

Pictures or screenshots of a live lesson must never be shared on online.

Livestream and Recorded Lessons

Staff and pupils may not have used video conferencing services. Provide clear user guidance that explains how to use them securely, and check that the service works as described.

It is strongly advised that you ask your teachers to test that the video conferencing service is working before using it for real session. They should be familiar with how to use the security features listed below such as familiarising themselves with controls such as approving participants in the lobby, removing participants from the call and muting individuals.

Ideally it is advised a second member of staff be present to protect both the staff member and the children.

Teachers should:

- Only use platforms specified and authorised by senior managers
- Sit against a neutral background
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- Wear suitable clothing like they would for school
- Double check that any other tabs they have open in their browser would be appropriate for a child to see, if they're sharing their screen
- Language must be professional and appropriate, including any family members in the background. This is especially important if you are working from home
- Be clear that a classroom standard of behaviour is expected from all
- Be sensitive to the needs of individual students, including those with sight or hearing impairments, and children who may be sensitive to certain topics or issues that may arise during the livestream
- To treat the details explaining **how to join the meeting** as if it is as sensitive as the **meeting itself**
- Ensure they have a stable connection to avoid disruption to lessons, as far as is possible
- Always remain aware that they can be heard.
- Not meet children for 1:1s, groups only
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Give consideration to pupils arriving late and whether this will be allowed / how this will be managed.
- Decide whether you'll let pupils use chat functions within the lesson. Like any chat function, it could lead to bullying, or be a distraction from learning.

In addition, it is worth agreeing ground rules; creating safe spaces and explaining these as the introduction to each session. Examples may be who can speak. If this is the first time that classes are delivered online, it may take some time in becoming familiar with the new environment.

Parents should be asked to ensure:

- Pupils are in a shared space in their house, rather than in their bedroom.
- Pupils dress in clothes suitable for school, whilst this does not need to be school uniform, it should be appropriate – as should the clothing of anyone else in the room at the time.
- Pupils behave as they would in school
- Who'll also be there - be mindful that other children might see or hear them and anything in the background. Alternatively, you might still want to ask for pupils to be on mute with webcams off, to cut risks.
- Pupils use the necessary equipment and computer programs as intended.
- Pupils and parents do not record, store, or distribute video material without permission.
- They have a stable connection to avoid disruption to lessons, as far as is practicable
- Pupils always remain aware that they are visible.
- Pupils know ways to report any concerns about behaviour whilst online

Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

Recording of Live Sessions

Ideally it is advised a second member of staff be present to protect both the staff member and the children.

It is advised that the staff member leading the sessions makes a recording so there's something to go back to later on if you need to, and keep a log of who's doing video calls, who participated and when. Check that parents are happy with you making recordings first – ensuring they are aware it is for school records only.

Staff should record, the length, time, date and attendance of any sessions held and overview of content. In addition, staff supporting remote learning must record whether any safeguarding issues were noted. If concerns were reported/observed, staff will record the detail of this and the date/time these were shared with the DSL as per normal safeguarding reporting processes.

Contacting children at home via Telephone or Video Call

Staff might need to contact children individually, for example to support a welfare check or to give direct feedback on a piece of home learning. **In all cases make sure parents are aware and agree to the communication.**

Staff should only contact children during normal school hours, or at times agreed by the school leadership team (DfE, 2020).

Make sure someone else at school is aware, and keep a record of the date and time of each call

Have a parent there at the child's end, and have the phone on speaker phone

Any one-to-one sessions, for example pastoral care meetings, should be risk assessed and approved by the school's leadership team (DfE, 2020). Make sure staff know what safeguarding measures to take if they are having a one-to-one conversation with a child.

Use parents' or carers' email addresses or phone numbers to communicate with children, unless this poses a safeguarding risk.

Use school accounts to communicate via email or online platforms, never teachers' personal accounts.

Make sure any phone calls are made from a blocked number so teacher's personal contact details are not visible. Either use an app like 3CX that will route calls through your school's number rather than their own, or block their number so parents don't see it. (Give parents a heads-up of what time you'll be calling if you're blocking numbers, so they're more likely to pick up.)

If possible, have another member of staff on the call. If this isn't possible, discuss with SLT recording the call, with parents' permission. Explain you're recording for school records only.

If staff members are accessing families' contact details at home, ensure they comply with the Data Protection Act 2018.

Parent Contact with School

Each school are responsible for communicating with parents their approaches for contacting staff and when they'll get replies.

Safeguarding

Online or offline, effective Safeguarding requires a whole-school approach. Planning for online or distance learning activities should include the school's safeguarding team as part of the planning process. Ensure online tuition follows best practice (e.g. 2 members of staff involved) and is in-line with the School's Safeguarding Policy.

Remind all your staff of your safeguarding and child protection policy and procedures. Staff need to follow the trust staff code of conduct which includes Guidance for safe working practice' for professionals working in education settings.   This guidance is also part of each school's child protection policy. All staff should have confirmed via Compliance Manager that they have read both these key documents.

Check that everyone is able to contact your nominated child protection lead and deputy if they have any concerns about a child. This may be because:

- a staff member sees or hears something worrying during an online lesson

- a child discloses abuse during a phone call or via email.

Remind students of who they can contact within the school for help or support.

Your nominated child protection lead should keep a note of any contact numbers they may need while the school is closed, for example children's social care and the local police.

In addition, during the period of remote learning, the school are advised to maintain regular contact with parents to:
- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Using Google Drives, including the features of G Suite for Education (e.g. Google Classroom and Google Meet)

If teachers are uploading resources to an *open* Google Drive

Make sure there's nothing that can identify pupils in the resources, like their names or comments addressed specifically to them, as anyone with the link can view what's in an open Drive.

Note: if you're using a Google Drive as part of G Suite for Education, you don't need to worry about this. By default, your school's Google Drive will only be visible to users in your school.

If you're using Google Classroom to set work and communicate

Decide:
- Whether you'll allow pupils to post and comment in the communication 'Stream', or disable this function for them (see below)
- What they can talk about in posts and comments, if allowed to

(If you disable pupil comments in the 'Stream', pupils will still be able to respond to feedback from their teacher on work they've handed in – they just won't be able to post on the 'Stream' page.)

To disable pupil comments in the 'Stream':

1. Open your class in Google Classroom
2. Click 'Settings' (the cog icon)
3. Scroll down to 'General'
4. Click the drop-down option to the right of 'Stream' and select 'Only teachers can post or comment'
5. Click 'Save'

If you allow pupils to comment, tell them they should only talk about school work in the 'Stream' and that you may 'mute' them, i.e. stop them from posting or commenting (see below), if they post anything that's inappropriate or bullying in nature.

Give parents the chance to opt out of their child posting in the 'Stream' too. If they opt their child out, mute them.

To 'mute' a pupil:

1. Click on a class in Google Classroom
2. Click 'People'

3. Next to the pupil you want to mute, check the box
4. Click 'Actions' > 'Mute'
5. Click 'Mute' again to confirm

To delete inappropriate or bullying posts or comments (you'll still be able to view them if you need to use them as evidence – see below):

1. Go to the class
2. Find the post or comment you want to delete
3. Click 'More' (the 3 dots) > 'Delete'
4. Click 'Delete' again to confirm

To view deleted posts and comments:

1. Go to the class
2. Click 'Settings' (the cog icon)
3. Next to 'Show deleted items', click 'Show' to toggle on
4. Hide the deleted items again by clicking 'Hide' to toggle off
5. Click 'Save' to save your changes and return to the 'Stream' page

If you're using Google Chat and Google Meet

Decide whether you'll let pupils communicate in Google Chat (previously called Google Hangouts). Like any chat function, it could lead to bullying, or be a distraction from learning.

To turn off Google Chat, you need to be an administrator. From the Admin Console Homepage, go to:

1. Apps > G Suite > Hangouts Chat
2. Click 'Service status'
3. To turn chat off for everyone, click 'Off for everyone'
4. Click 'Save'

This will turn off the chat function for everyone – staff and pupils. If you just want to turn it off for pupils, follow the more intricate steps here (particularly step 5).

To record in Google Meet: (You'll need to be using the computer version of Meet to record.)

1. In the meeting, click 'More' (the 3 dots) > 'Record meeting'
2. Wait for the recording to start
3. When you finish, click 'More' > 'Stop recording'
4. Click 'Stop recording' again to confirm
5. Wait for the recording file to be generated and saved to the Meet Recordings folder. The meeting organiser and the person who started the recording will also get an email with the recording link

If you're using Google Meet for live streams

In 'view-only' Google live streams, pupils will be <u>automatically muted and won't be visible</u>, so you don't need to worry about what other adults in their homes might do that gets caught on camera.

If you <u>schedule meetings</u> in Google Calendar or Gmail, pupils won't be able to rejoin once the final attendee has left. This means pupils won't be able to rejoin for their own private calls.

Using Office 365 Education (e.g. Microsoft Teams)

The following link explains how to set up a meeting using Teams.

<u>https://www.hertsforlearning.co.uk/blog/how-use-microsoft-teams-education-how-set-video-calls-people-outside-your-organisation?fbclid=IwAR32vkt3oLnyTFwPyKvdjotZYk2zaowYiSCma0y_qWDcMHjGN1jpWYFqAC4</u>

This will generate an email invitation to all invited attendees, containing a link via which they can join the meeting.

If you're using Microsoft Teams decide whether you'll let pupils use chat in Microsoft Teams.

Like any chat function, it could lead to bullying, or be a distraction from learning.

To disable chat for pupils, you need to create a '<u>messaging policy</u>' in Teams and then assign it to pupils.
First, create your new messaging policy:

1. Log in to the Microsoft Teams <u>admin centre</u>
2. Click 'Messaging policies' on the left-hand side
3. Click 'New policy' and give it a name (e.g. 'Disable chat')
4. Select the 'Chat' setting, and turn it off
5. Click 'Save'

Then, assign this policy to pupils:

1. Log in to the admin centre
2. Click 'Messaging policies' on the left-hand side
3. Click on the policy you've just made, then 'Manage users'
4. Search for the user you want to add, click on their name, and then click 'Add'
5. Repeat step 4 until you've added all of your pupils
6. Click 'Save'

To <u>record</u> in Microsoft Teams:

1. In the meeting, click 'More options' (the 3 dots) > 'Start recording'
2. Wait for the recording to start (you'll get a notification saying 'Recording has started')

3. When you finish, click 'More options' > 'Stop recording'
4. Wait for the recording to be saved in Microsoft Stream (whoever started the recording will get an email notification when it's ready to watch)

If you're using Microsoft Teams for live streams

> To <u>record</u> a live event in Teams, check the 'Recording available to producers and presenters' setting when you schedule your live stream. You can make the recording available for pupils too, by checking 'Recording available to attendees'. The recording will be available for 180 days after the event ends.

> To disable chat for pupils, uncheck the 'Q&A' setting when you schedule your live stream.

Using Cisco WebEx Meetings

To host a meeting in a WebEx meeting you need a different APP – called WebEx Meetings. This, like WebEx teams can be downloaded to a PC (it can be downloaded to a mobile but the functionality is limited). You will need your own WebEx site. To create a site go to https://www.webex.com/ and click on 'start for free'. Once you sign up you will receive an email that includes your own WebEx site. From your site you can start meetings immediately or schedule them.

Go to your site – and check you are on modern view (icon towards top right)
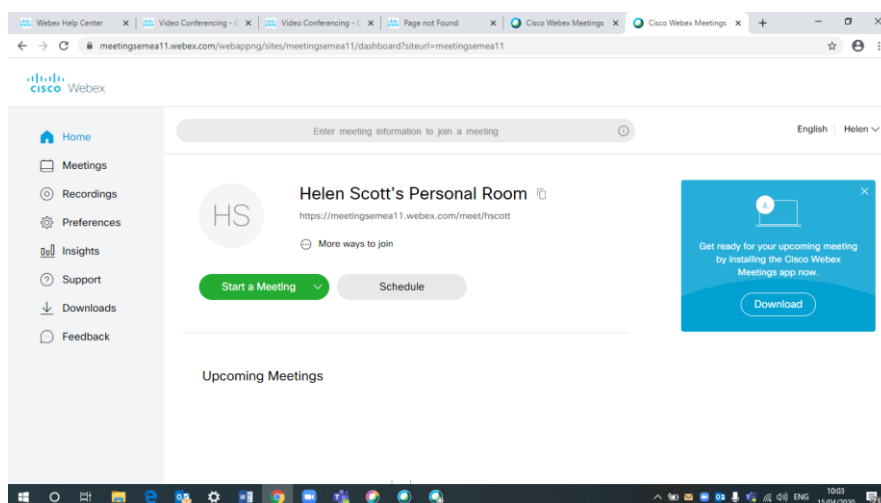
Your screen will look like this.

It is safer to schedule a meeting than to start one. Click the 'schedule' button.

- Make sure your meeting title is generic, not identifying an individual/ confidential info
- Make a note of your password – you will need to send it separately to participants
- Enter attendees as prompted on screen
- Click the drop down for 'show advanced options'
- Then click scheduling options

- Make sure you tick the 'exclude password' box – for added security this will now NOT send the password with the invite; you will have to send it separately.
- Make sure also that nobody can join before the host (you)
- By default, participants cannot video the meeting and you cannot change this – only you would have that facility.
- Minutes may be taken as would be at a LAC.
- You can use the meeting options and attendee privileges to suit you

To participate in a WebEx meeting – there are 2 options.

1) You need to go to the WebEx website https://www.webex.com and click 'join'. The screen will prompt the participant to ensure a meeting number and access code that you have sent to them – in separate emails as explained above - inviting them to the meeting.
2) The participant can download the APP – they can then click 'join meeting' in the email you sent them and they will be asked for the password

Some useful links for further guidance

https://help.webex.com/tutorial/section/Cisco%20Webex%20Meetings

https://www.youtube.com/watch?v=5WywiTZEIS8

Please ensure best practice is followed for secure meetings. Cisco produce guidance which should be used to ensure security.

https://support.webex.com/LocalizedUpgrades/2014/bestpractices/best_practices_for_secure_meetings_admin.pdf

https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

## Security that must be adhered to for devices used.

Guidance here is taken from https://secure.school/. We strongly recommend that school-issued devices, set up by trained professionals are used where possible. Allowing staff to use their own devices can introduce significant cyber security and data protection risks. This is because the technology used on personal devices can differ greatly to that used on technology designed and set up securely by IT departments and service providers. Some of these risks will expose the school to cyber-attacks. Others can expose the school to fines and other consequences of data breaches.

Where this is not possible, for example where a school device fails, the school need to ensure the following safety information has been shared with meeting participants and that they have actioned the guidance within it.

1. **Antivirus – it is crucial that antivirus software is installed and up to date**
   Antivirus is software that is designed to detect, stop and remove viruses and other kinds of malicious software (malware). Malware can harm your devices and the data stored on them by:
   ➢ Stealing your data
   ➢ Making your data inaccessible
   ➢ Erasing your data
   ➢ Infecting other devices

Microsoft Windows

Close down all applications so that you can see your desktop wallpaper.

Click on the Start Menu, type 'windows security' and press return on your keyboard.

Take a look at the 'Virus & threat protection' section. A green tick means antivirus is installed and updated.

Apple Mac

Close down all applications so that you can see your desktop wallpaper.

On your keyboard, press command-shift-A keys together to bring up the list of installed applications.

We've gathered a list of well-known antivirus products. Check if any of these are in your installed applications.

2. **The operating system must be up-to-date**
   Companies that make the main software for your computer, such as Microsoft and Apple, regularly release updates (called patches) that fix security vulnerabilities. We call the process of installing these updates patching. Patching is the single most important thing you can do to secure your devices. Most of the time updates will install automatically. Sometimes though, this isn't the case and therefore it's important to perform a manual check
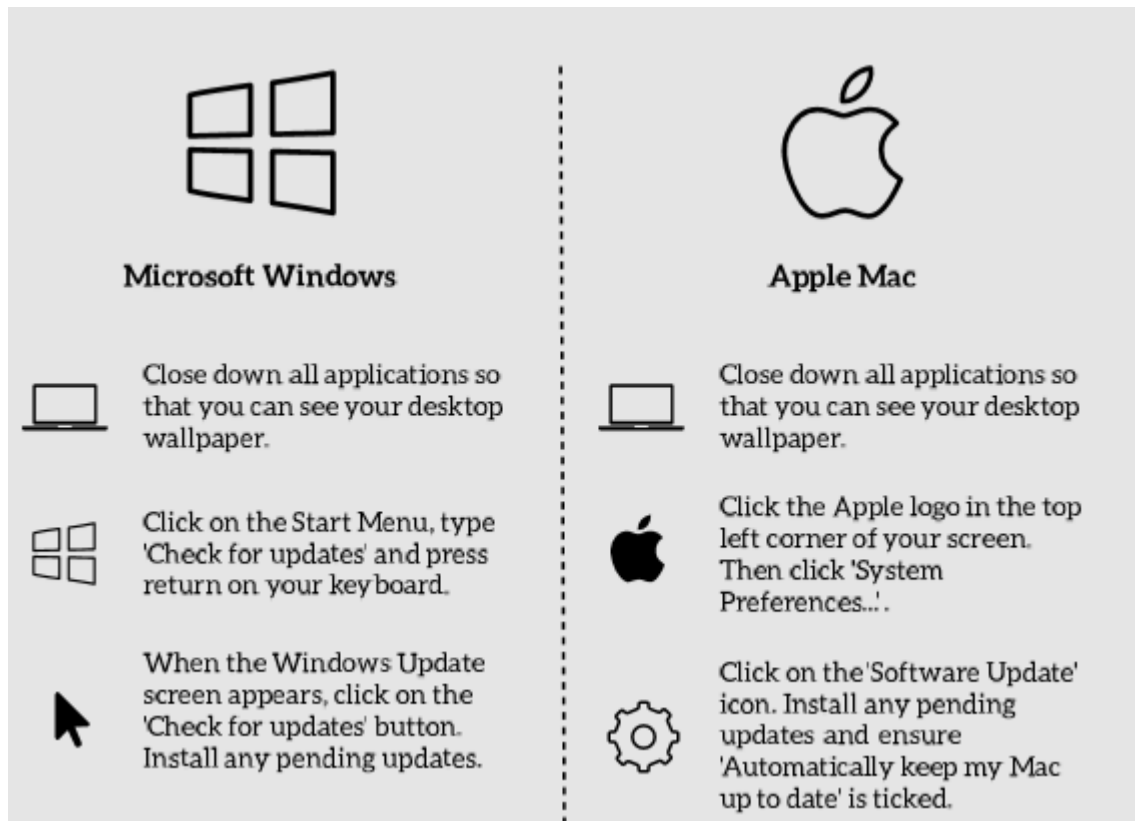
Microsoft Windows	Apple Mac
Close down all applications so that you can see your desktop wallpaper.	Close down all applications so that you can see your desktop wallpaper.
Click on the Start Menu, type 'Check for updates' and press return on your keyboard.	Click the Apple logo in the top left corner of your screen. Then click 'System Preferences...'.
When the Windows Update screen appears, click on the 'Check for updates' button. Install any pending updates.	Click on the 'Software Update' icon. Install any pending updates and ensure 'Automatically keep my Mac up to date' is ticked.

3. **Ensure that the device has a strong password, passcode or PIN**
   Passwords, passcodes and PINs are secrets that only the user of a device should know. They are used to prevent unauthorised access to devices and the data stored on them. It's important that strong passwords are used on devices to protect against password-type attacks.
   If you've used a password before, there is a chance it has already been compromised. If you re-use the same password across multiple device or online accounts, if a cybercriminal finds out your password, they have access to them all

   How to Create the Password
   Be creative and think of three random words. Add a number and a special character. eg. BeatCanvasSand29@

   How to Set the Password
   If you don't currently need a password to access your device, or you've used your device's password for anything else, set the new password

Microsoft Windows

Close down all applications so that you can see your desktop wallpaper.

On your keyboard, press ctrl-alt-del at the same time. Click 'Change a password'.

Enter your old password (leave blank if there was no password before). Enter the new, strong and unique password into the 'New password' box and once again in the 'Confirm password' box. Press return on your keyboard.

Apple Mac

Close down all applications so that you can see your desktop wallpaper.

Click the Apple logo in the top left corner of your screen. Then click 'System Preferences...'.

Click on the 'Users & Groups' icon, select your account under 'Current User' on the left and click on 'Change Password...'.

Enter your old password (leave blank if there was no password before). Enter the new, strong and unique password into the 'New password' box and once again in the 'Verify' box. Click 'Change Password'.

4. Check that the device has a firewall enabled

Devices that can connect to networks often come with software that prevents unauthorised connections. This software is called a firewall. A firewall can stop cybercriminals from connecting to your device and can help protect against the spreading of malware.

Most of the time, the built-in firewall is already enabled. However, for various reasons it is sometimes disabled, leaving the device at risk.

Microsoft Windows

Close down all applications so that you can see your desktop wallpaper.

Click on the Start Menu, type 'windows security' and press return on your keyboard.

Take a look at the 'Firewall & network protection' section. A green tick means your firewall is enabled.

Apple Mac

Close down all applications so that you can see your desktop wallpaper.

Click the Apple logo in the top left corner of your screen. Then click 'System Preferences...'.

Click on the 'Security & Privacy' icon, then the 'Firewall' tab. If the Firewall is turned off, click 'Turn On Firewall'.

Useful links and further relevant resources

Online safety

Children and young people are likely to spend more time online due to social distancing. Talk to them regularly about the benefits and risks of the online world and give them space to ask questions and talk about anything that worries them.

> Find out more about e-safety for schools
> Take our online training about keeping children safe online

Some helpful resources for Parents

- A4 poster of top tips for parents to keep their children safe online during corona closures (there are video explainers on Twitter or Facebook).

- Video chatting: a guide for parents and carers of Primary Aged Pupils

- A new DigiSafe Daily downloadable worksheet is available every day during term time at digisafedaily.lgfl.net for parents or teachers of primary pupils to download and use at home.

NSPCC - https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

Video conferencing services: security guidance for organisations

https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations reviewed April 2020

For office 365 products - https://www.ncsc.gov.uk/collection/saas-security/product-evaluations/office-365

For g-suite products https://www.ncsc.gov.uk/collection/saas-security/product-evaluations/g-suite

NCSC Poster – Video Conferencing, using services securely – click the image to link to the PDF which may be useful for staff and parents

The UK Safer Internet Helpline includes further useful guidance for schools -

https://swgfl.org.uk/services/professionals-online-safety-helpline/

The Edublogger - a useful blog giving insight into how educators around the world are approaching school closures. The blog has compiled, curated, and built on some common themes and ideas to create this extensive guide.

https://www.theedublogger.com/teaching-online-school-closures/#video

The Education Endowment Foundation

https://educationendowmentfoundation.org.uk/covid-19-resources/best-evidence-on-supporting-students-to-learn-remotely/

https://educationendowmentfoundation.org.uk/public/files/Campaigns/Distance_Learning_Rapid_Evidence_Assessment_Protocol.pdf

There is also a review on the Early Intervention Foundation website – a webinar too https://www.eif.org.uk/report/covid-19-and-early-intervention-evidence-challenges-and-risks-relating-to-virtual-and-digital-delivery

<mark>Annex A</mark>

<mark>TO DO before using</mark>

- **<mark>Add School header</mark>**
- **<mark>Check or change text highlighted in yellow</mark>**

Name of pupil:	
Name of parent:	

Consent to participate in video conferencing

School is developing new ways of working to provide children with engaging learning opportunities, especially at times when they may need to be learning at home. There are occasions where we believe it is in the best interests of your child to learn collaboratively with their classmates and teachers, using video conferencing. We will only ask your child to participate in video conferencing with your consent.

The online safety of your child is our priority. <mark>Name of School</mark> follows the guidance set out by The Aspire Educational Trust for safety in remote online video and telephone communication with pupils and parents. This guidance has been developed following expert advice from organisations such as DfE, NSPCC and UK Safer Internet Centre and can be found on our website by clicking this <mark>link [add hyperlink link]</mark>.

The video platform/s the school will be using is/are <mark>[name platform/s].</mark>

How we will keep your child safe

- The technology we use will have been risk assessed by the school prior to setting up any video conferences.
- Video conferences will only be hosted on school accounts and devices.
- Staff who are hosting meetings will have completed online safeguarding training and received training to understand the platform features that maximise security.
- Meetings will be set up with the recommended level of security as detailed in the trust guidance including <mark>[add in here settings for your platform such as waiting rooms, passwords, no screen sharing].</mark>
- There will be no 1:1 video conferencing.
- Your child will always be invited to join a secured meeting using the e-mail address we have for you as their parent. We ask you to keep the invitation information confidential and request you do not share it with others.
- We will inform you of the intended activity when we invite your child to attend a conference.
- Staff will agree the ground rules for creating a safe online space at the start of each video conference. This will include reminding children not to share private information and who they should tell if they see or hear anything upsetting or inappropriate.
- We may record the meeting so that the session can be reviewed if there is a need to. Recordings are strictly for the school's use only. The lawful basis for recording and retaining the meeting is public task as it is solely for the purposes of safeguarding children.
- Recordings will be kept securely for one month after the event in accordance with our data protection and records management policies. Recordings will only be accessed by authorised staff.
- **Pictures or screenshots of a live lesson will not be shared on online.**
- A log of the content overview, date, time and participants of all video conferences will be kept.
- <mark>[Add in anything else that you wish parents to know]</mark>

How you can keep your child safe

We ask you to ensure:

- Your child is in a shared space in your house, rather than in their bedroom.
- Your child is dressed in clothes suitable for school, whilst this does not need to be school uniform, it should be appropriate.
- Your child is reminded to behave as they would in school.
- You check there is nothing in the background that may be distracting or private.
- You check your internet connection is secure.
- You or your child do not record, store, or distribute video material without permission.

Providing your consent

The school will only invite your child to attend a livestream video conference with your consent.

This form is valid for participation in all video conferences until your child leaves our school.

Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional video conference platform will be used.
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil should not participate in livestream video conferences.
- Changes to parental consent.

Parents have the right to withdraw their consent at any time. Where you would like to amend or withdraw your consent, you must submit your request in writing to the headteacher. A new form will be supplied to you to amend your consent accordingly.

Please read the information above thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No'.

I provide consent for:	Yes	No
My child to participate in livestream video conferences		

Declaration

I, _____ (name of parent), understand:

- Why my consent is required.
- The reasons why **name of school** uses livestream video conferencing.
- The safeguarding measures school will take.
- The safeguarding measures I will take.
- I have provided my consent above as appropriate, and the school will involve my child in livestream video conferencing in line with my requirements.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the headteacher.

Name of parent: _____

Signature: _____

Date: _____