
NUNNEY FIRST SCHOOL



ONLINE SAFETY POLICY

Rationale

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of online safety;
- work to empower the school community to use technology, including the Internet, as an essential tool for life-long learning.

This policy is used in conjunction with other school policies, and has been developed by a working group, including representatives from all groups within the school.

The Online Safety Policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.

Scope of policy

This policy applies to all members of the school community including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school.

Keeping Children Safe in Education (September 2019¹) sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety (para 88)
- appropriate filters and appropriate monitoring systems are in place (para 87)
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach (page 98)

1

The school will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The implementation of the Online Safety Policy will be monitored by an Online Safety working group, meeting as deemed appropriate e.g. 3 times a year and reporting to the Local Governing Body annually.

The impact of the policy will be monitored by the Online Safety working group by looking at:

- the log of reported incidents
- the Internet monitoring log
- surveys or questionnaires of learners, staff, parents and carers
- other documents and resources
- future developments.

Roles and responsibilities

The Headteacher and governors oversee the safe use of technology when children are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online safety and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The Online Safety Leader will work with the Headteacher, who is also the Designated Safeguarding Lead (DSL), to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials including: extremism and radicalisation; inappropriate online contact with adults; potential or actual incidents of grooming and cyber-bullying.

An Online Safety working group will work with the Online Safety Leader to implement and monitor the Online Safety Policy and Acceptable Use Policies (AUPs). This group is made up of the Online Safety Leader, Designated Safeguarding Lead (DSL), a governor, a TA, IT technician and pupils. Pupils are important members of this group and contribute their knowledge and use of technology. The group meets three times per year.

Role	Responsibility
Governors	<ul style="list-style-type: none"> • Monitor the effectiveness of the Online Safety Policy • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to the Local Governing Body • Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online
Headteacher	<ul style="list-style-type: none"> • Ensure that all staff receive suitable CPD to carry out their online safety roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents

	<ul style="list-style-type: none"> • Ensure that there is a progressive online safety curriculum in place • Ensure that there is a system in place for monitoring online safety • Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or a pupil • Inform the CEO of The Bath and Mendip Partnership Trust about any serious online safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review online safety with the school's technical support
Online Safety Lead	<ul style="list-style-type: none"> • Lead the Online Safety working group • Coordinate work with the school's Designated Safeguarding Lead (DSL) • Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of Online Safety policies and documents • Lead and monitor a progressive online safety curriculum for pupils • Ensure all staff are aware of the procedures outlined in policies relating to online safety • Provide and/or broker training and advice for staff • Attends updates, subscribe to appropriate newsletters and liaise with the Trust technical staff • Meet with the Headteacher and Online Safety Governor to discuss incidents and developments
Teaching and Support Staff	<ul style="list-style-type: none"> • Participate in any training and awareness raising sessions • Read, understand, sign and act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or concerns to the Online Safety Leader / Designated Safeguarding Lead (DSL) and check this has been recorded • Provide appropriate online safety learning opportunities as part of a progressive online safety curriculum • Model the safe, positive and purposeful use of technology • Monitor the use of technology in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct, especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a 'critical incident'
Pupils	<ul style="list-style-type: none"> • Read, understand, sign and act in accordance with the Pupil AUP / agreed class Internet safety rules • Report concerns for themselves or others

	<ul style="list-style-type: none"> • Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	<ul style="list-style-type: none"> • Endorse (by signature) the Pupil AUP • Discuss Online Safety issues with their child(ren) and monitor their home use of technology including tablets, mobile phones and games devices, and the Internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Headteacher of any online safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to the school on social media
Technical Support Provider	<ul style="list-style-type: none"> • Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network using an approved password • Maintain and inform the Headteacher of issues relating to filtering • Keep up to date with online safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Leader/Headteacher for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows)
Community Users	<ul style="list-style-type: none"> • Sign and follow the Guest/Staff AUP before being provided with access to school systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP • Use the Online Compass tool to review online safety

Education of pupils

'Children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.'

Keeping Children Safe in Education 2019

A progressive, planned online safety education programme is in place. This meets the requirements of DfE guidance, 'Teaching Online Safety In Schools²' (June 2019). Online safety teaching is delivered through discrete lessons and is reinforced across the curriculum, for all children in all year groups. This allows for key teaching points and core concepts to be regularly revisited. Breadth and progression is ensured through referring to the UK Council for Internet Safety's (UKCCIS) framework, 'Education for a Connected World'³ and is implemented using the 2Simple Purple Mash computing scheme of learning,

² <https://www.gov.uk/government/publications/teaching-online-safety-in-schools>

³

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/680356/Education_for_a_Connected_World2.pdf

supplemented by Somerset's ActiveBYTES scheme.

Within this:

- Key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset ActiveBYTES and Purple Mash schemes of learning.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where Internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use. Processes are in place for dealing with any unsuitable material that is found via Internet searches.
- Pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- The Online Safety Leader maintains and passes on knowledge of current concerns to be included within learning experiences.
- Pupils are provided with opportunities to influence the online safety curriculum.
- Pupils will read, discuss and sign an AUP for their class at the beginning of each school year. This will be shared with parents and carers.
- Pupils are educated to recognise and respond appropriately to different forms of bullying, including cyber-bullying. They are given opportunities to support each other.
- Online safety resources are differentiated to support the youngest learners and SEN learners to establish appropriate habits for responsible use of technology.

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children in managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children.

- Providing regular, easy to access support materials e.g. on Class DOJO and the online safety page of the school website.
- Raising awareness through activities planned by pupils.
- Inviting parents to attend activities such as Online Safety Week, online safety assemblies or other meetings as appropriate.
- Providing and maintaining links to up to date information on the school website.

Education of the wider school community

The school provides information about online safety to organisations using school facilities such as Nunney Pre-School and members of the wider community. This information is provided through newsletters and the school website. It includes online safety messages targeted to parents, grandparents and other relatives.

Training of Staff and Governors

There is a planned programme of online safety training as part of the overarching safeguarding approach. This is in line with the requirements of 'Keeping Children Safe in Education 2019' (paragraph 84 and page 98) for all staff and governors, to ensure they understand their responsibilities as outlined in this DfE statutory guidance and the AUPs.

This includes:

- All staff knowing the Designated Safeguarding Lead and the Online Safety Lead and their responsibilities.
- An annual audit of the online safety training needs of **all** staff.
- All new staff and governors receiving online safety training as part of their induction programme.
- Providing information to supply and student teachers on the school's online safety procedures.
- The Online Safety Leader receiving regular updates through attendance at training sessions and by reviewing regular online safety newsletters from the Local Authority.
- This Online Safety Policy and its updates being shared and discussed in staff meetings and in meetings of the Local Governing Body.
- The Online Safety Leader providing training within safeguarding training, and as specific online safety updates and reviews.
- The Online Safety Leader providing guidance as required, to individuals and seeking Trust advice and support on issues and matters arising.

- Staff and governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772.

Online bullying

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by: telling a trusted adult; online bully box, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

Pupils, staff and parents/carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of online bullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents/carers will be required to work with the school to support the approach to online bullying and the school's online safety ethos.

Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the school's Behaviour Policy and AUP and may include:

- The bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content.
- Internet access being suspended at the school for a period of time.
- The parent/carers of pupils being informed.
- The police being contacted if a criminal offence is suspected.

Sexting

The school will follow UKCCIS⁴ advice on how to respond to an incident. We will provide appropriate support for sexting incidents that take place in and out of school. Within school, any device that has an illegal image of a child under 18, or is suspected of having

4

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf

such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority. This will also be reported to the CEO of The Bath and Mendip Partnership Trust.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the Internet on the premises. Appropriate levels of filtering are in place through a managed filtering service that includes terms related to terrorism. Appropriate monitoring of Internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Technical Infrastructure

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP. This document is held by The Bath and Mendip Partnership Trust as the employer.

The school ensures, when working with technical support providers, that the following guidelines are adhered to:

- The school ICT systems are managed in ways that ensure that the school meets online safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations and other devices from accidental or malicious attempts, which might threaten the security of the school systems and data with regard to:
 - ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our business continuity plan
 - the downloading of executable files by users
 - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
 - the installing of programs on school devices unless permission is given by the technical support provider, Headteacher or Computing Leader
 - the use of removable media e.g. memory sticks, by users on school devices - see Data Protection Policy for further detail

- the installation of up to date anti-virus software.
- Access to the school network and Internet will be controlled with regard to:
 - users having clearly defined access rights to school ICT systems through group policies
 - users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is in place to monitor activity)
 - staff users being made aware that they are responsible for the security of their username and password, which they are required to change every 60 days; they must not allow other users to access the systems using their log on details
 - the 'master/administrator' passwords are available to the Trust Director of Business as well as the Trust Computing Team
 - users must immediately report any suspicion or evidence that there has been a breach of security
 - an agreed process being in place for the provision of temporary access of "guests" e.g. trainee or supply teachers, visitors, onto the school system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this Online Safety Policy.
- The Internet feed will be controlled with regard to:
 - the school's responsibility⁵ to "ensure appropriate filters and appropriate monitoring systems are in place. Children are safeguarded from potentially harmful and inappropriate online material." Keeping Children Safe in Education 2019
 - Foundation Stage and Key Stage 1 pupils' access will be supervised, with access to specific and approved online materials
 - Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities
 - requests from staff for sites to be removed from the filtered list being approved by the Headteacher and logged⁶
 - user-based filtering used to provide differentiated access for staff and pupils

⁵ <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

⁶ <https://www.somerset.org.uk/sites/edtech/eSafety/Filter/Benefit%20Analysis%20request%20for%20unfiltering%20a%20website.pdf>

- filtering issues being reported immediately.
- The IT system of the school will be monitored with regard to:
 - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems
 - online safety incidents being documented and reported immediately to the Online Safety Leader or Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with in accordance with school policies.

Data Protection

The Bath and Mendip Partnership Trust's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- At all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates.
- Use personal data only on secure password protected computers and other devices.
- Ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data.
- Provide staff with secure equipment/services to store or transfer data e.g. remote access, OneDrive, SharePoint school portal, encryption and secure password protected devices.
- Remove data in line with The Bath and Mendip Partnership Trust's Data Retention Policy.
- Ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead (Headteacher) and that relevant staff understand the full requirements of Data Protection Act 2018.
- Complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely.

Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- Build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound.
- Ensure verifiable permission⁷ from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use.
- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose.
- Make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed.
- Ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs.
- Not publish pupils' work without their permission and the permission of their parents or carers.
- Only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the Trust's Data Retention Policy.
- In accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video

⁷ <https://nunneyfirstschool.co.uk/wp-content/uploads/2018/05/TPT-Photograph-Policy-NUNNEY-April-2018.pdf>

images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school.

- Make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection Regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people.

Communication (including use of Mobile Devices and Social Media)

A wide range of communications technologies increases effective administration and has the potential to enhance learning. The school will:

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email and other communication tools alongside online safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this is required
- protect the identities of multiple recipients by using bcc in emails.

with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate, educationally focussed sites that will be moderated by the school
- control access to social media and social networking sites in school

- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Headteacher
- ensure that any digital communication between staff and pupils or parents/carers is open, transparent and professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice⁸, being careful about subjects discussed online
- staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts
- register concerns e.g. recording in Online Safety log, regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them online
- inform the staff that in the case of a 'critical incident' they should not make any comment on social media without the permission of the Headteacher.

with respect to personal devices (including consideration of Keeping Children Safe 2019⁹)

- inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times)

⁸ DfE Cyberbullying Advice for headteachers
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf and Teaching Standards 2012
<https://www.gov.uk/government/publications/teachers-standards>

⁹
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/830121/Keeping_children_safe_in_education_060919.pdf page 97

- ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes
- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Headteacher
- check any use of a personal device for an education purpose (where permission has been given) only uses the school's Internet connection, on the school site
- remind all that personal devices should be pin code or fingerprint protected and not discoverable by third parties
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- provide a mobile phone for activities that require them
- challenge staff and visitors when there is suspected misuse of mobile phones or devices
- when pupils are allowed personal devices in school, they are used within the school's Behaviour Policy and pupils understand they can be asked to account for their use
- use the right to collect and examine any pupil device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection.

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones/wearable technology in school		✓						✓
Use of mobile phones/wearable technology in lessons				✓				✓

Use of mobile phones/wearable technology in social time	✓							✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of personal devices including wearable technology		✓					✓	
Use of 'always on' voice activated technology				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat facilities, forums and closed groups in apps	✓						✓	
Use of messaging apps	✓						✓	
Use of social networking sites including live broadcasting	✓						✓	
Use of blogs	✓					✓		
Use of Twitter	✓					✓		
Use of video broadcasting e.g. YouTube		✓						✓

With respect to video conferencing and remote teaching:

Procedures:

- Every meeting should be documented - a spreadsheet should be kept of the meetings that were held, with whom, for how long, and for what purpose.
- Have a very specific focus e.g. annual reviews or music therapy. Staff can't set up video meetings without authorisation.
- Communicate with parents about it through Class Dojo or email. Explain that you will be using the conferencing app for a specific activity, at this time, on this day. Give them the option to include their child if they wish. Consent is assumed if they choose to login to the meeting. Where possible, the meeting should be password protected and a waiting room used to check who is joining.
- Hosts will consider safety features e.g. muting webcams and microphones if there are any concerns about what pupils are discussing and locking the meeting five minutes after the scheduled start time. The parent should be in the same room as their child during the video session. Pupils must be presented as if they are in the classroom, and if the teacher thinks the pupil is inappropriately dressed they should remove them from the session.

Safeguarding:

- Remind staff that there should be no direct communication between the teacher and pupils outside of the video meeting - all communication is between the parent and teacher.
- The staff member should set up accounts using a school email address, not their personal email address.
- No sessions with pupils should be recorded by staff unless the school considers there is a safeguarding risk or concerns about content/conduct - this must be discussed with Headteacher.
- All staff undertaking such lessons are expected to be appropriately dressed and in a room that does not have continuous distractions.
- The staff member should be aware that any safeguarding concerns or disclosures should be responded to and reported in the same way as they would if they had occurred in the school.

Data security:

- After the session, staff should delete their session cookies to avoid any data mining from video conferencing apps.

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances, the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material.

The school provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

The school will follow Somerset's incident flowchart to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where

this is appropriate. Should content being reviewed include images of child abuse, the investigation will be referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns such as breaches of filtering, online bullying, extremism, radicalisation, illegal content.
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage online safety incidents in accordance with the School Behaviour Policy where appropriate.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Advisor or Local Authority Designated Officer (LADO).

<p>If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Advisor to communicate to other schools in Somerset.</p> <p>Should serious Online Safety incidents take place, the following external persons and agencies should be informed:</p>	<p>Education Safeguarding Adviser Jane Weatherill Via Somerset Direct where pupil involved</p> <p>Local Authority Designated Officer (LADO) Anthony Goble Via Somerset Direct where staff involved</p> <p>CEO of The Bath and Mendip Partnership Trust via their PA, Sam Vernau svernau@thebathandmendippartnershiptrust.com</p> <p>Police</p>
--	--

The police will be informed where users visit Internet sites, make, post, download, upload,

data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false.

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation (p 17)):

- child sexual abuse images
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity including radicalisation and terrorism
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet.

In addition, the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)		✓		
Online gaming (non-educational)				✓
Online gambling				✓
Online shopping / commerce			✓	
File sharing (using p2p networks)			✓	

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy. Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, ticks may appear in more than one column.

The ticks in place are actions which must be followed.

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff action re filtering / security etc	Inform parents / carers	Removal of network / Internet access rights	Warning	Further sanction e.g. detention / exclusion
	Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓			✓		✓
Unauthorised use of non-educational sites during lessons	✓				✓		✓	

Unauthorised use of mobile phone / wearable technology / personal tablet	✓				✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓				✓		✓	
Unauthorised downloading or uploading of files	✓				✓		✓	
Allowing others to access school network by sharing username and passwords	✓	✓			✓		✓	
Attempting to access or accessing the school network, using another pupil's account	✓	✓			✓		✓	✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓		✓	✓			✓
Corrupting or destroying the data of other users	✓	✓		✓	✓	✓		✓
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓			✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓		✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓			✓			✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓	✓		✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive, pornographic or extremist material	✓	✓	✓		✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓		✓	

Sanctions: Staff

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, marks may appear in more than one column.

The marks in place are actions which must be followed.

Incidents:	Refer to Headteacher	Refer to Trust Business Director/Trust CEO	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	L				✓
Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email	✓				✓		

Unauthorised downloading or uploading of files	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓		✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	P	✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff	✓	✓	P				✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	✓	✓	L				✓
Breach of the school Online Safety policies in relation to communication with learners	✓	✓					✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils?	✓	✓	L				✓
Actions which could compromise the staff member's professional standing	✓	✓			✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓			✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise	✓	✓	L/P			✓	✓
Breaching copyright or licensing regulations	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓					✓

Date adopted by the Governing Body: 8th June 2020

Signed by Chair of Governors: *Sue Thomas*

This policy will be reviewed triennially or more regularly in response to significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The next anticipated review date is: June 2023