Weare Academy Church of England First School

Online Safety Policy

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. It also applies to both staff and pupil use of technology for remote/online learning as part of a blended approach and during any school closures (partial or full) e.g. during a national/local lockdown or due to severe weather.

Keeping Children Safe in Education 2020 sets out specific responsibilities for governing bodies to ensure:

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

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.

This Online Safety Policy should be read in conjunction with the following other linked school policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Management Policy
- Acceptable Use agreements
- Prevent Policy
- Biometric Data Policy
- Relationships Education Policy
- Virtual Learning Policy
- Social Media Policy
- GDPR Policy and staff guidance document
- Data Protection Policy, agreements and other documentation (e.g. Privacy Notice and permission forms for data sharing, image use etc)

Schedule for development, monitoring and review

The implementation of the Online Safety Policy will be monitored by an Online Safety working group, meeting termly and reporting to the Governors 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 and learners 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 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.

KCSIE 2020 states that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)". The Online Safety Lead will work with the Headteacher, 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 Lead to implement and monitor the Online Safety Policy and AUPs (Acceptable User Policies). This group is made up of Online Safety Lead, Designated Safeguarding Lead (DSL), governor, member of support staff, technician, and pupils. Pupils are an important part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	• Approve the Online Safety Policy • Monitor the effectiveness of the Online Safety Policy[1] • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Online Safety Lead to carry out regular monitoring and report to Governors • 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
Head Teacher	• 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 • Ensure that there is a progressive Online Safety curriculum in place • Ensure that there is a system in place for monitoring Online Safety

[1] Online safety in schools and colleges: Questions from the Governing Board

	• Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil • Inform the local authority 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 • Work with the DSL, Online Safety Lead and Data Protection Officer to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and online safety requirements
Online Safety Lead	• Lead the Online Safety working group • Coordinate work with the school's Designated Safeguarding Lead (DSL) and PSHE/RSE lead • 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 • Work with the PSHE/RSHE and Computing Leads to embed and monitor a progressive Online Safety curriculum for pupils, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum • Work with the DSL, Headteacher and Data Protection Officer to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and online safety requirements • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Provide and/or broker training and advice for staff • Attend updates, subscribe to appropriate newsletters and liaise with the LA Online Safety staff and technical staff • Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments • Complete the 360 Degree Online Safety review
All Teaching and Support Staff	• 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 (within or outside school) to the Designated Safeguarding Lead (DSL) and check this has been recorded and actioned • 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, including Online/Remote Learning • Be mindful of the additional safeguarding considerations required if delivering Online/Remote Learning • 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
PSHE/RSE lead	• Work with the Online Safety and Computing Lead to embed and monitor a progressive Online Safety curriculum for pupils, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum

Computing lead	• Work with the Online Safety and PSHE/RSE Leads to embed and monitor a progressive Online Safety curriculum for pupils, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum
Pupils	• Read, understand, sign and act in accordance with the Pupil AUP appropriate use of technology agreement • Report concerns for themselves or others • Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss appropriate, healthy, safe use of technology and 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	• 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 • Support the school to ensure that platforms selected by the school for Online/Remote learning meet safeguarding and online safety requirements • Maintain and inform the Senior Leadership Team 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 Lead for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	• Sign and follow the Staff AUP before being provided with access to school systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP

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 2020

A progressive planned Online Safety education programme takes place in line with 'Teaching online safety in schools', through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UKCCIS Education for a Connected World framework and is implemented through the use of Somerset 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 scheme of work

- 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 and processes are in place for dealing with any unsuitable material that is found in 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 lead 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 write and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers

- pupils are educated to recognise and respond appropriately to ‘different forms of bullying, including cyber-bullying’ and given opportunities to support each other

- a continuous provision map is used with 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 with 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 newsletter items and appropriate support materials
- raising awareness through activities planned by pupils and staff
- providing and maintaining links to up to date information on the school website

Training of Staff and Governors

There is a planned programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2020 for all staff and governors to ensure they understand their responsibilities, as outlined in this, 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, NQTs will be supported to complete the UKCIS Online Safety Audit Tool.

- providing information to supply and student teachers on the school's Online Safety procedures

- the Online Safety Lead receiving regular updates through attendance at training sessions and by reviewing regular Online Safety newsletters from the LA

- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings

- the Online Safety Lead providing training within safeguarding training and as specific online safety updates and reviews

- the Online Safety Lead providing guidance as required to individuals and seeking LA support on issues

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

Peer on Peer abuse

All members of staff are made aware that children can abuse other children (often referred to as peer on peer abuse). Children are encouraged to talk to members of staff if they feel they are the victim or perpetrator, or if they are aware of peer on peer abuse. This abuse may include:

Cyberbullying

Cyberbullying (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 policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- 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 and 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 and action taken 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 and 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 schools Behaviour Policy or 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 and carers of pupils being informed

  - the police being contacted if a criminal offence is suspected

Sexting

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

Sexual harassment, including upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats
- upskirting

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL). The Designated Safeguarding Lead (DSL) will record the incident(s) and the actions taken in line with DfE Guidance and advice from Somerset Local Authority and/or the police as necessary.

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 the Exa-Networks Internet Service Provider and their education based managed filtering service which 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.
The school ensures, when working with our technical support provider 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 or Computing/ICT coordinator

    - the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data 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 put 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 for all systems are available to the Headteacher and kept securely in an agreed place

- 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 responsibility[2] to "ensure appropriate filters and appropriate monitoring systems are in place. Children are safeguarded from potentially harmful and inappropriate online material." Keeping Children Safe 2020

  - 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

[2] https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

- requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged[3]

- user based filtering used to provide differentiated access for staff and pupils

- 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 Lead or Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with immediately in accordance with school policies

Data Protection

The school'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

[3] https://www.somerset.org.uk/sites/edtech/eSafety/Filter/Benefit%20Analysis%20request%20for%20unfiltering%20a%20website.pdf

- 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 eg Wessex Learning Trust Office 365 portal with email and One Drive, SharePoint school portal, encryption and secure password protected devices

- remove data in line with the school’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 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 *(read in conjunction with the Social Media Policy)*

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 permission 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 schools 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 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

Social Media

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school/academy name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation
- **Administrator/Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school/academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/academy, including volunteers or parents.

Monitoring

School/academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school/academy social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be

considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload pupil pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school/academy are outside the scope of this policy.
    - Where excessive personal use of social media in school/academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - The school permits reasonable and appropriate access to private social media sites.
- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.**
    - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
    - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.

- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school/academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Communication

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

with respect to email and other online communication tools (e.g. Microsoft Teams, Google Meet):

- ensure that the school uses secure business systems for communication
- ensure that personal information is not sent via unsecure systems
- ensure that governors use secure systems
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that communications will be monitored by the school
- inform users what to do if they receive online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email and other communication tools alongside safe, healthy appropriate use of technology and online safety issues through the scheme of work and implementation of the AUP

- only publish official staff email addresses where this required

- protect the identities of multiple recipients by using bcc in emails

with respect to Online/Remote Learning opportunities e.g. Microsoft Teams, Zoom, Google Classroom, Tapestry etc.:

- develop a strategic approach to Blended Learning which enables online/remote learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school

- when selecting online learning platforms, first consider data protection.

- 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 access to platforms will be password protected and run with approval from the Senior Leadership Team

- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content

- discuss the use of online/remote learning as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice[4], being careful about subjects discussed online

- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use (in or out of school) and raise with their parents and carers

- support staff to deal with the consequences of hurtful or defamatory posts about them online

[4] 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

with respect to personal devices (including consideration of Keeping Children Safe 2020 and in conjunction with the Social Media Policy):

- 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)

- 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 SLT

- 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 / code of conduct, 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

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times in certain are	Allowed for selecte staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
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		✓						✓
Use of blogs		✓				✓	✓	
Use of Twitter		✓						✓
Use of video broadcasting e.g. YouTube	✓					✓	✓	
Use of live video streaming e.g. Microsoft Teams, Zoom	✓					✓	✓	

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. Where content being reviewed is suspected or known to include images of child abuse, the investigation will be referred to the Police immediately and no further access will be made by the school to the material.

- 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 Service or Local Authority Designated Officer (LADO).

If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Service to communicate to other schools in Somerset. Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Education Safeguarding Service *Via Somerset Direct where pupil involved* Local Authority Designated Officer (LADO) *Via Somerset Direct where staff involved*

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:

- 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 in certain areas	Acceptable for nominated users	Unacceptable
Online gaming (educational)	✓			
Online gaming (non-educational)	x			x
Online gambling	x			x
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	Refer to class teacher / tutor	Refer to Head of Department / Hea of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network /internet acce rights	Warning	Further sanction eg detention / exclusion
Deliberately producing, 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:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff fc action re filtering etc	Disciplinary action: Warning	Disciplinary action: Suspension	Disciplinary action: Other
Deliberately producing, accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	L,P				
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		✓	✓		✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		✓	✓			✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		✓	✓	L		✓		
Breech of the school Online Safety policies in relation to communication with learners		✓	✓	L		✓		
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		✓	✓	L		✓	✓	
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise		✓	✓	L		✓	✓	
Breaching copyright or licensing regulations	✓							
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓	✓	

Monitoring and evaluation

The implementation of this policy will be monitored by the Headteacher and the Online Safety Lead.

The review of this policy will take place:	Autumn 2022
Approved by Governors:	(date)
Signed by Chair of Governors:	*Mr M. O'Connor*
Signed by Headteacher:	*Miss D. Mawdsley*