Online Safety Policy

KINGSMOOR PRIMARY SCHOOL

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 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 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.

The Online Safety policy approved by Governing body in the Summer term 2020

The next review date is: Summer term 2021

CONTENTS

Policy Aims

Kingsmoor Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and report/record any incident, where appropriate

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 online bullying, which may take place out of school, but are linked to membership of the school.

Keeping Children Safe 2019 [1] (para 87) sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety
- appropriate filters and appropriate monitoring systems are in place

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.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and Health Education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835733/Keeping_children_safe_in_education_2019.pdf

National Curriculum computing programmes of study. At Kingsmoor, we follow the Elim scheme of work written by Somerset County Council.

LINKS TO OTHER POLICIES

This online safety policy is linked to our:

- Safeguarding policy
- Anti-bullying policy
- Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure

SCHEDULE FOR DEVELOPMENT, MONITORING AND REVIEW

The Implementation of the Online Safety policy will be monitored by Online Safety representative reporting to the Governors.

The impact of the policy will be monitored by Online Safety representative by looking at (when relevant):

- 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 take action 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.

Mr Neil Thompson, Deputy Headteacher, is the appointed Online Safety Leader and deputy designated safeguarding lead and will have an overview of the serious child protection issues to 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 online bullying).

An Online Safety representative, Mrs Bruna Berridge will work with the Online Safety Leader to implement and monitor the Online Safety policy and AUPs (Acceptable User Policies). This representative is a member of the Kingsmoor Community.

Role	Responsibility
Governing Board	- The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. - **All governors will:** - Ensure that they have read and understand this policy

	- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet - Approve and review the effectiveness of the Online Safety Policy - Delegate a governor to act as an online safety link. The governor who oversees online safety is Bruna Berridge. - **The delegated Online safety Governor will:** - Co-ordinate a termly meeting with the Online safety lead to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). - Online Safety Governor works with the Online Safety Leader to carry out termly 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 and Senior Leaders	- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school - Ensure that all staff receive suitable CPD to carry out their Online Safety roles including online risks of extremism and radicalisation (Prevent training) - 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 - 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 - Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
Designated Safeguarding Lead	- Details of the school's DSL (and deputies) are set out in our child protection and safeguarding policy as are relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular: - to ensure that staff understand this policy and that it is being implemented consistently throughout the school - Work with the computing lead, Mr Neil Thompson, and other staff, as necessary, to address any online safety issues or incidents - Ensuring that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy - Ensuring that any incidents of cyber-bullying are logged on My concern and dealt with appropriately in line with the school Behaviour and Anit-bullying policies.

	- Updating and delivering staff training on online safety - Liaising with other agencies and/or external services if necessary - Providing regular reports on online safety in school to the headteacher and governing board
Online Safety Leader (Mr Neil Thompson)	- With support from the School Business manager. Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material - Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly - Working with school's technical support provider (Computeam) to conduct a full security check and monitoring the school's ICT systems on a termly basis as well as blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files - When relevant and where appropriate, log, manage and inform others of Online Safety incidents and how they have been resolved in line with this policy 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 - Attend updates and liaise with the LA Online Safety staff and technical staff - Meet with the Online Safety Governor termly to discuss incidents and developments

Teaching and Support Staff	All staff, including contractors and agency staff, and volunteers are responsible for: - Maintaining an understanding of this policy - Implementing this policy consistently - Act in accordance with the AUP and this policy - Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use - Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy - Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school anti-bullying and behaviour policies - Participate in any training and awareness raising sessions - Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum and respond - 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	- Read, understand sign and act in accordance with the Pupil AUP and the agreed class Internet rules - 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	Parents are expected to: - Notify a member of staff or the headteacher of any concerns or queries regarding this policy - Ensure their child has read, understood and agreed to the terms on the Pupil AUP and endorse this with their signature - 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 the 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 - Parents can seek further guidance on keeping children safe online from the following organisations and websites: - What are the issues? - UK Safer Internet Centre - Hot topics - Childnet International - Parent factsheet - Childnet International
Visitors and members of the community	Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. They will be expected to agree to the terms on acceptable use.
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. - 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 Leader 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

EDUCATING PUPILS ABOUT ONLINE SAFETY

'Governing bodies and proprietors should ensure that 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

Pupils will be taught about online safety as part of the curriculum and how online safety should be implemented throughout the schools curriculum. From September 2020 **all** schools will have to teach Relationships and Health Education in primary schools.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant.

Kingsmoor will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured and is implemented through the use of Somerset ActiveBYTES schemes of work[2].

Within this:

- key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons

- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset Active Bytes 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, 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 extreme and 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

- pupils are provided with opportunities to influence the online safety curriculum

- pupils will write and sign an AUP for their class [*which might be agreed class rules*] 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 online bullying' – see links to school leaflet for parents regarding bullying.

- 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 and regular newsletter and website updates;

[2] https://staffonly.somerset.org.uk/sites/edtech/SitePages/e-Safety/ActiveBYTES.aspx

- 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;

- Online safety guidance and information will also be made available during parents evenings.

- providing and maintaining links to up to date information on the school website

- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Education of wider school community

If appropriate, the school provides information about Online Safety to organisations using school facilities, local play groups and nurseries and members of the wider community which where appropriate include:

- details about the Online Compass review tool

- Online Safety messages targeted to grandparents and other relatives

CYBER-BULLYING

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also our school's anti-bullying and behaviour policies.)

Preventing and addressing cyber-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 policy on anti-bullying and behaviour. Details of the procedures in place to support anyone in the school community affected by online bullying can be found in the anti-bullying policy.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes at an age appropriate level and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes relationships and health education, and other subjects where appropriate.

All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

The school also sends information on cyber-bullying to parents via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Headteacher, or the deputy headteacher in her absence, will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

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 will be encouraged 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 using My Concern.

The school will follow procedures to investigate incidents or allegations of online bullying. As stated in our Anti-bullying policy, 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 Anti-bullying, 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

Definition

The act of sending sexually explicit photos, messages, voicemails, videos, etc., either via phone, computer, webcam or other device.

The school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an intimate sexting image 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 will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

TRAINING OF STAFF AND GOVERNORS

There is a planned programme of Online Safety training 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 on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

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

- the Online Safety Leader receiving regular updates through attendance at SWGfL and LA 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 Leader providing training within safeguarding training and as specific online safety updates and reviews

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

- staff and governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 477

.

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 which includes terms related to terrorism. 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, work stations 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 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 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 (apart from possibly Foundation Stage and Key Stage One pupils) being provided with a 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 are available to the Headteacher and School Business Manager and kept in the school safe
    - 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. All "guests" must sign the staff AUP and are made aware of this Online Safety policy
    - the school's responsibility[3] to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" Keeping Children Safe 2016
    - 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 Senior Leadership Team and logged[4]
    - 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

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

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

- 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 immediately in accordance with school policies

DATA PROTECTION

The schools Data Protection Policy provides full details of the requirements that need to be met in relation to the 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

- store or transfer data using approved services such as remote access, the Somerset Learning Platform (SLP), 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

- 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 AND VIDEO IMAGES

Photographs and video taken 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[5] 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

[5] https://staffonly.somerset.org.uk/sites/edtech/eSafety/Policies/Pupil_images_consent%20form.doc

- when using digital images, staff ~~to~~ 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

COMMUNICATION (INCLUDING USE OF SOCIAL MEDIA)

A wide range of communications technologies have 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 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 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 advice[6], 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 senior management team

with respect to personal devices (including consideration of Keeping Children Safe 2018[7])

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Headteacher

- 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 Senior Leadership Team

- 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

- inform all that personal devices should be password protected

- 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

- pupils are not allowed to bring mobile phones into school at any time.

---

[6] 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

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707761/Keeping_Children_Safe_in_Education_-_September_2018.pdf page 93

- maintain the right to collect and examine any phone 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			
Communication Technologies	Allowed	Allowed at certai times	Allowed for select staff	Not allowed	Allowed	Allowed at certai times	Allowed with sta permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on school owned mobile phones or other camera devices for educational purposes eg iPad	✓						✓	
Use of personal devices		✓						✓
Use of personal email addresses in school, or on school network			✓					✓
Use of school email for personal emails			✓					✓
Use of chat rooms / facilities			✓				✓	
Use of messaging apps			✓				✓	
Use of social networking sites			✓				✓	
Use of blogs			✓				✓	
Use of Twitter			✓					✓
Use of video broadcasting eg Youtube			✓					✓

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 flowcharts 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 then the monitoring will be halted and 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 an appropriate log. All reported incidents will be dealt with and actions recorded

- The designated Safeguarding Lead 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)

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. Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Education Safeguarding Advisor Jane Wetherall *Via Somerset Direct where pupil involved* Local Authority Designated Officer (LADO) *Via Somerset Direct where staff involved* Police

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 user	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:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg withdrawal of privileges (playtime) / 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 / digital camera / other handheld device	✓	✓			✓		✓	
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	✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓	✓		✓
Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg withdrawal of privileges (playtime) / exclusion
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 or instant message 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 or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓		✓	

SANCTIONS: STAFF

Incidents:	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P	Refer to Technical Suppo Staff for action re filtering	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,P		✓	✓	✓

Incidents:	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P	Refer to Technical Suppo Staff for action re filtering	Warning	Suspension	Disciplinary action
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	✓	✓			✓		
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	✓	✓		
Incidents:	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(F	Refer to Technical Suppo Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access offensive or pornographic material	✓		L	✓	✓		✓
Breaching copyright or licensing regulations	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓		In some cases		✓	✓	✓