Tatworth Primary School

ONLINE SECURITY POLICY

Ratified by:	Full Board of Directors
Date:	17 September 2020
Agenda Item	7.5
Next Review:	Autumn Term 2021
Signed by the Chair	
Date	17 September 2020

Distribution:	OneDrive Website
Source:	SCC

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

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

This policy is used in conjunction with other school policies.

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.

Contents

Scope of policy

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

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

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

- children are taught about online safety (para 93)
- appropriate filters and appropriate monitoring systems are in place (para 92)
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach (para 89)

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

Schedule for Development, Monitoring and Review

The implementation of the Online Safety Policy will be monitored by an Online Safety Leader/Co-ordinator, teacher of ICT (Jonathan Goodman) who will report any issues immediately to SLT. A general report will also be presented to the Board annually.

The impact of the policy will be monitored by:

- 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 Directors 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.

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

The Online Safety Leader, will implement and monitor the Online Safety Policy and AUPs (Acceptable User Policies) [Annexed below]. Pupils are an important part of the monitoring process, the school council will be asked to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Directors	• Monitor the effectiveness of the Online Safety Policy • Delegate a director to act as Online Safety link • Online Safety Leader to carry out regular monitoring and report annually to Directors • 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	• 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 • 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
Online Safety Coordinator	• Coordinate work with the school's Designated Safeguarding Lead(DSL) • Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate • Use an audit[1] to annually review Online Safety with the school's technical support • 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, subscribe to appropriate newsletters and liaise with the LA Online Safety staff and technical staff • Meet with Senior Leadership Team and Online Safety Director to discuss incidents and developments

[1] https://staffonly.somerset.org.uk/sites/edtech/Subscriber%20Only/Questions%20for%20Technical%20Support%20v4.pdf

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 to the Online Safety Leader / Designated Safeguarding Lead (DSL) and check this has been recorded • Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum • Model the safe, positive and purposeful use of technology • Monitor the use of technology in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand, sign and act in accordance with the Pupil AUP / 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	• Endorse (by signature) the Pupil AUP • Discuss Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Headteacher of any Online Safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to the school on social media
Technical Support Provider **(Soltechit)**	• 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

Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP

Education of pupils

'An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology.'

Keeping Children Safe 2020

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 through reference to UKCCIS Education for a Connected World framework[2] and is implemented through the use of Somerset ActiveBYTES scheme[3].

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 coordinator 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

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/680356/Education_for_a_Connected_World2.pdf
[3] https://www.somerset.org.uk/sites/edtech/SitePages/e-Safety/ActiveBYTES.aspx

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
- inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate
- providing and maintaining links to up to date information on the school website

Training of Staff and Directors

There is a planned programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2020 (paragraph 92 and page 24) for all staff and directors 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 directors receiving Online Safety training as part of their induction programme
- providing information to supply and student teachers on the school's Online Safety procedures
- the Online Safety Leader receiving regular updates through attendance at training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Director meetings
- the Online Safety Leader providing training within safeguarding training and as specific online safety updates and reviews
- the Online Safety Leader providing guidance as required to individuals and seeking LA support on issues
- staff and directors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772

Online bullying

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

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

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

Pupils, staff and parents 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 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 for Learning 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 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.

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. 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, 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 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 are available to the Headteacher 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. 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[4] 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
    - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged[5]
    - 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 Leader or Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with immediately in accordance with school policies

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

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

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
- 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 remote access, 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

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[6] 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

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

- 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 Mobile Devices and Social Media)

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

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that directors 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 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[7], 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 2020)

- inform staff that personal devices 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
- remind all that personal devices should be password protected 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
- challenge staff and visitors when there is suspected misuse of mobile phones or devices
- 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

[7] 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

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 certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones/wearable technology in school		Y						Y
Use of mobile phones/wearable technology in lessons				Y				Y
Use of mobile phones/wearable technology in social time	Y							
Taking photos on mobile phones or other camera devices				Y				Y
Use of personal devices including wearable technology		Y						
Use of 'always on' voice activated technology				Y				Y
Use of personal email addresses in school, or on school network				Y				Y
Use of school email for personal emails				Y				Y
Use of chat facilities, forums and closed groups in apps				Y				Y
Use of messaging apps		Y						Y
Use of social networking sites including live broadcasting				Y				Y
Use of blogs		Y						Y
Use of Twitter		Y						Y
Use of video broadcasting e.g. YouTube		Y						Y

Assessment of risk

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

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

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

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

Reporting and Response to incidents

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

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded
- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage Online Safety incidents in accordance with the School Behaviour for Learning 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.	Education Safeguarding Adviser Jane Weatherill *Via Somerset Direct where pupil involved* http://www.supportservicesforeducation.co.uk/Services/3246
Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Local Authority Designated Officer (LADO) Anthony Goble *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 use	Unacceptable
Online gaming (educational)			Yes	
Online gaming (non-educational)				Yes
Online gambling				Yes
Online shopping / commerce			Yes	
File sharing (using p2p networks)			Yes	

Sanctions: Pupils

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

The ticks in place are actions which must be followed.

Incidents	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staf for action re filtering / securit	Inform parents / carers	Removal of network /internet access rights	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓		✓		
Unauthorised use of non-educational sites during lessons		✓			✓		
Unauthorised use of mobile phone / wearable technology / personal tablet		✓			✓		
Unauthorised use of social networking / instant messaging / personal email		✓			✓		
Unauthorised downloading or uploading of files		✓			✓		
Allowing others to access school network by sharing username and passwords	✓				✓		
Attempting to access or accessing the school network, using another pupil's account	✓						
Attempting to access or accessing the school network, using the account of a member of staff		✓			✓		
Corrupting or destroying the data of other users		✓			✓		
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature		✓			✓		
Continued infringements of the above, following previous warnings or sanctions			✓		✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓			✓		
Using proxy sites or other means to subvert the school's filtering system		✓			✓		
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓		
Deliberately accessing or trying to access offensive, pornographic or extremist material		✓			✓		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓		

Sanctions: Staff

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

The marks in place are actions which must be followed.

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Sta for action re filtering etc	Follow Disciplinary Procedure
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓		✓		✓
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		✓		✓		✓
Breech of the school Online Safety policies in relation to communication with learners		✓				
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils?		✓	✓			
Actions which could compromise the staff member's professional standing		✓		✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓		
Using proxy sites or other means to subvert the school's filtering system		✓	✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓		✓

Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise		✓		✓		✓
Breaching copyright or licensing regulations		✓	✓			✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓

Pupil Acceptable Use of Technology Policy

Technology is a great tool to support learning, find information and to communicate and share with others.

The School encourages its appropriate, effective and safe use. All users of technology in the school must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities

I understand that the school will monitor my use of computers and other technology.

I understand that I have rights and responsibilities in using technology and will follow the class agreed rules when using technology including the internet.

I understand that the school may investigate incidents that cause upset or harm taking place outside school.

I recognise if I misuse technology, it has an effect on others and consequences for me.

I will report any suspected misuse or problems to a trusted adult in the school.

I will think about the ways I use technology so that it will not affect my physical or mental health.

Online bullying

I understand that the school will not accept bullying in any form.

I will be careful to check that anything I write or say in documents, messages or online is not offensive or could cause hurt or embarrassment.

I understand that I should report any incidents of bullying.

Use of internet

I will not try to access sites that are blocked or that are unsuitable for use in school.

I will carefully check information I use for my learning.

I will report any worrying or damaging materials I come across.

Personal mobile devices

I will only use personal mobile devices when I have permission from by my teachers.

Name _____

Signed _____

Class _____ Date _____

PARENT/CARER ACCEPTABLE USER POLICY
FOR PUPILS' USE OF TECHNOLOGY AND THE INTERNET

The school uses technology, including the internet, to support the curriculum wherever this is appropriate. Pupils are taught computing and about effective and responsible use of technology and the internet. Pupils are given guidelines and taught how to be careful and considerate in their use of technology and the internet and how to maintain a balance between this and other activities.

The school may use approved blogs, emails, picture galleries and other tools to help with educating your child. Children and staff will always use responsible and caring language online.

Pupils will:

- only use technology including computers and mobile devices when they have been told that they can.
- only use the school technology for those activities which they have been given permission.
- be told about online bullying and what to do if it happens.
- use only the user names and passwords for which they have permission.
- not download and use material or copy and paste content which they do not have consent to use.
- not attempt to search for, view, upload or download any inappropriate or unsuitable material.
- inform a member of staff if they have accidentally found inappropriate or unsuitable content.
- use responsible and caring language in communicating with others.
- be helped to maintain a balance between the use of technology and other activities.
- be helped to discuss their use of the internet especially sites where there is communication with others (e.g. social networks).
- only use mobile devices when directed by staff
- be encouraged to talk with their parents or carers about the rules for the safe use of the internet.
- be made aware that the school may investigate incidents that happen outside of school but could affect life in school.

Misuse of technology may result in:

- a ban, temporary or permanent, on the use of the internet / technology resources at school
- action in line with the school's behaviour policy
- parents/carers being informed about an incident and actions taken

Parents and carers work in partnership with the school when they:

- discuss online safety issues with their children and work to build responsible use of technology
- work with the school in promoting positive use of technology and the internet
- inform the school if they think there is an online safety issue related to the school
- raise concerns about the school through the appropriate channels

Please ask a member of staff if you have questions about any part of this document. **Please sign below and return this form to the school.**

- I have read and am happy with the description of the school's technology and internet use.
- I will work with the school to help my child develop appropriate use of technology.
- I am happy for my child to experience the internet use described.

Pupil Name (PLEASE PRINT) _____ Class _____

Name of Parent or Carer (PLEASE PRINT) _____

Signature of Parent or Carer _____ Date _____

Staff and Volunteer Acceptable Use Policy

School Policy
This Acceptable Use Policy reflects the school Online Safety Policy. The school will ensure that staff and volunteers will have access to technology to enable efficient and effective working enabling learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy
This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally and professionally.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the school Online Safety Policy
- report any suspected misuse or concerns to the Online Safety Leader / Designated Safeguarding Lead
- monitor technology activity in lessons, extracurricular and extended school activities, including awareness of any access to extremist views
- model the safe and effective use of technology
- 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 especially at the time of a Critical Incident

Education

I agree to:

- provide age-appropriate online safety learning opportunities as part of a progressive online safety curriculum; and reinforce the learning throughout the school's curriculum
- respect copyright and educate the pupils to respect it as well
- teach about the need for using responsible and caring language when communicating with others

Training

I agree to:

- participate in online safety training
- request training if I identify an opportunity to improve my professional abilities

Online bullying

I agree to:

- ensure the school's zero tolerance of bullying. In this context, online bullying is seen as no different to other types of bullying
- report any incidents of bullying in accordance with school procedures

Sexting

- I will secure and switch off any device discovered with a sexting image and report immediately to the safeguarding lead.
- I will not investigate, delete or resend the image.

Prevent

- I will continually develop children's ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure

I understand that the school will monitor my use of computing devices and the internet. Unless I have permission, I will not try to by-pass any of the technical security measures that have been put in place by the school which include:

- the proxy or firewall settings of the school network
- not having the rights to install software on a computer
- not using removable media e.g. memory sticks

Passwords

- I will only use my own passwords
- I will never log another user onto the system using my login

Filtering

- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately

Data Protection

- I understand my responsibilities towards the data protection regulations and will ensure the safe keeping of personal and sensitive personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up and kept secure.
- If I believe there has been a loss of personal or sensitive data, I will immediately report it to the Data Protection Lead in the school.

Use of digital images, video and sound

- I will follow the school's policy on using digital images, video and sound, especially in making sure that only those pupils whose parental permission has been given are published.
- I will not use personal devices for taking or sharing digital images or sound.

Communication

- I will be professional in all my communications and actions when using school technology systems.
- I understand that I need to be open and transparent in all my communications.

Email

- I will use the school provided email for all business matters.
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media and Personal Publishing

- I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work. These will never be my personal accounts.
- I will check with the SLT before I use sites/apps with learner log ins to ensure that any pupil personal data is being held securely.
- I will follow the online safety policy concerning the personal use of social media, never publishing disparaging or harmful comments or expressing extreme views. These are considered to bring the school into disrepute
- I will not post any comments about the school, any pupil, employer or colleagues on any personal social networking and publishing accounts
- In the event of a Critical Incident, I will not post any comments online.

Personal devices

- I will not use personal devices during contact time with pupils.
- I will not use my personal devices to contact pupils or parents.
- I will only use the school's filtered and monitored broadband access while in school

Reporting incidents

- I will report and record any incidents relating to online safety to the Online Safety Leader / Designated Safeguarding Lead and check actions taken have been recorded
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use technology and will apply sanctions if they do not follow the rules.
- I understand that if I misuse the School technology systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name _____

Signed _____

Date _____

i-Pad Acceptable User Agreement for Staff

Data Protection and Security

- Do not set up your personal email address on the School device.
- Do not link up personal third party apps or services, such as Dropbox or other storage; on-demand TV; other media streaming services without approval from Mrs Hart
- Do not to sign into personal social media accounts, e.g., Twitter; Facebook; LinkedIn without approval from Mrs Hart
- You must not jailbreak the school mobile device, or otherwise hack, or tamper with them.

User Responsibility

- Your iPad device must be in a protective case at all times.
- Handle your device with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.
- Only approved cleaning materials can be used to clean your device, such as laptop or tablet sprays and cloths.
- Do not keep or leave your iPad unattended in vehicles.
- Keep your iPad safe and secure at all times. You should know where your iPad is at all times.
- Ensure your battery is charged, and ready for school use each and every morning.

Lost, Damaged, or Stolen Devices

- If your device becomes lost or stolen, report it to Mrs Hart as a matter of urgency.
- If your device has become damaged, report it to Mrs Hart and hand over the device to them.
- You must not carry out repairs on any school-owned device.
- You must not solicit any individual or company to repair a school-owned device on your behalf.

Safeguarding and Online Safety

- All device usage is subject to the rules and guidelines of the school's online safety policy. Anyone in breach of this policy may be subject, but not limited to disciplinary action, confiscation, removal of content, or referral to external agencies.
- Do not tamper with iPad devices belonging to other members of staff. Anyone found trying to access another staff member's device or associated content will be subject to disciplinary action.
- If an iPad is found, return it immediately to Mrs Hart .
- Do not take photographs of others using your iPad without their express permission
- As with all other school devices, outlined within our ICT and Safeguarding policies, you are strictly forbidden from using your device to create, store, access, view, download, distribute, send, upload inappropriate content or materials.
- You are forbidden from utilising your iPad to partake in illegal activities of any kind.
- Do not use your iPad to post images, movies, or audio to a public facing part of the internet, without the express permission of all individuals imaged/recorded. Where this includes students, refer to the head teacher, and ensure that full permission has been received from the head, as well as parents/guardians before a post is made.
- School iPad and any content are subject to routine and ad-hoc monitoring by Mrs Hart.You must hand over your device upon request by any member of staff.
- You must ensure compliance with the online safety policy when using your iPad.

Personal Use

- Your iPad device is not permitted for personal use. It has been provided for work-related use only.
- Refer to the school's online safety policy for guidelines on utilising your iPad device to browse the internet outside of school.
- Do not grant access to anyone, unless expressly authorised to do so by the head teacher.
- Staff are prohibited from taking or storing personal photos/videos on school devices as these may be seen in school by students or other staff.

SIGNED:_____

NAME:_____

DATE:_____

Technician/Administrator

Acceptable Use Policy Extension

The school ICT Technician or person with administration rights is placed in an exceptional position of trust. Some of the duties that the Headteacher expects these people to complete could be against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the ICT technician to fulfil these duties.

Areas of concern are that:

- Files could be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, extremist, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.
- User accounts will need to be created and serviced meaning that there may be access to these accounts by the ICT technician.
- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of sensitive personal data including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.
- The ICT technician, through specific user names and passwords, has control (sometimes through remote workstations) to the school's network and this trust must not be abused.

Because of these areas of concern the ICT Technician should:

- be responsible for monitoring the school's network including the internet use of staff and pupils; and provide regular reports to the School Leadership Team.
- be given permission to access other user's files.
- protect the users by maintaining a filter for the school.
- be aware of the laws relating to the use of computers especially those around Computer Misuse, Data Protection, Prevent and sexting images, copyright and those referred to in the school's Online Safety Policy and AUPs.
- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.
- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information and the school's Prevent duty.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made and actions taken.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise including:
    - secure and switch off any device that is suspected of containing an intimate sexting image and report to safeguarding lead
    - never open websites that are suspected of having inappropriate material unless others are present
- have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has administration responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: _____

Signed: _____

Senior Member of Staff: _____

Date: _____

Regular Visitor Acceptable Use Policy

Visitors will

- apply appropriate standards when using computing devices in school including an awareness of Data Protection, Copyright laws, Prevent duty and reporting.
- only use personal devices, including a mobile phone during the working day in line with the policy for use by staff. This includes not using the device in the presence of child and not taking pictures or other recordings unless permission has been granted.
- not publish any information online that may be offensive to staff or pupils, or may bring the school into disrepute.

Logging in

- If you use the school's equipment, then request a guest log in.
- If you are using equipment that has been logged in by a member of staff they will always ensure they are in the room with you. They will lock the machine if they need to leave the room.
- If your service contract (Network/MIS support) allows you access to the system through team logins, inform the school of the purpose and how you will be accessing the system.

Internet Access and uploading

- The school's internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment:

- Make sure that you have permission from the school for its use
- Ensure it has up to date virus protection software installed.
- Ensure that you take appropriate precautions with trailing wires.
- Ensure that you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Wireless Access

- Where you have permission to use a personal smart device, you will use the school's wireless connection and will be provided with an authorisation key.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Downloading / Transferring files or documents

For all files

- Never transfer files unless you have permission, this must not be from a USB stick/external drive unless permission has been given by the headteacher.
- Make sure that you clearly state the purpose for transferring the files.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.
  (Note: permission will not be needed where existing service contracts, such as Network/MIS support, are in place. However, please indicate the type of work you will be doing).
- Transfer the file only over a secure email connection.

If you need to take pictures, video or record sound files then check that

- you have permission to capture these files.
- the staff/children have all given their permission for these images/voices to be used.
- you request permission in writing or through email should you intend to use these files in a public arena (website, blog etc.) or for financial gain.

Reporting

- Report any incidence of accidental viewing of inappropriate images or materials.
- Report any incidence of deliberate searching for inappropriate images or materials.
- Switch off and secure any device that you suspect of containing an intimate sexting image and report immediately to the school's safeguarding lead.

Name _____ Date _____

Occasional Visitors Online Safety Agreement

This list of statements has been developed to use with visitors that are only in school for a one-off occasion such as, a supply teacher that isn't being used regularly by the school, a visiting speaker or students that are helping for single days.

On signing the visitors' book, you agree to:

- only log onto the **school network** with the user name and password provided for you;
- inform the Headteacher or their representative if you intend to **use the internet**, asking permission before using any kind of social media with the children;
- not use a personal device, including your **mobile phone** during the working day (without permission from the headteacher);
- not use USB or external memory device without permission
- not take any **photographs** without the specific permission of the Headteacher or their representative;
- report any suspected **misuse or concerns** about online safety whether by pupils or staff, to the Headteacher or their representative before leaving the school;
- not take any **information on pupils or staff** off site unless specific permission has been given by the Headteacher or their representative;
- not **publish any information** online that may be offensive to staff or pupils, or may bring the school into disrepute.