Thurlbear CE VA Primary School
On-Line e Safety Policy

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 e Safety;
- work to empower the school community to use technology including the internet as an essential tool for life-long learning.

This policy is used in conjunction with other school policies and guidance. 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 on: _____

Signature of Chair of Governors: _____

The next review date is: _____

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 2016 [1]sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety (para 68);
- appropriate filters and appropriate monitoring systems are in place (para 67).

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

Schedule for Development, Monitoring and Review

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

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

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

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

Roles and responsibilities

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

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.

An Online Safety working group will work with the Online Safety Leader to implement and monitor the Online Safety Policy and AUPs (Acceptable User Policies). This group is made up of Online Safety Leader, Designated Safeguarding Lead (DSL), teacher, governor, member of senior leadership team and pupils through the school Values Group. Pupils are an important part of this group, to contribute their knowledge and use of technology. The Working Group meet on a termly basis.

Role	Responsibility
Governors	• Monitor the effectiveness of the Online Safety Policy. • Delegate a governor to act as Online Safety link. • Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to 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	• 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. • Use an audit[2] to annually review Online Safety with the school's technical support.
Online Safety Lead	• Lead the Online Safety working group. • Coordinate work with the school's Designated Safeguarding Lead(DSL). • Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate. • Lead the establishment and review of Online Safety policies and documents. • Lead and monitor a progressive Online Safety curriculum for pupils. • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety. • Provide and/or broker training and advice for staff.

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

	• Attend updates, subscribe to appropriate newsletters and liaise with the LA Online Safety staff and technical staff. • Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments.
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 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 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	• 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.

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;
- 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 from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use;
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites;
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose;
- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed;
- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs;
- not publish pupils' work without their permission and the permission of their parents or carers;

- only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the schools Data Retention Policy;

- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school;

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

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

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 required;

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

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[3], 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 Incident 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.

Mobile phones

- 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.

- 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.

- Inform all that personal devices should be password protected.

- 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

- 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.

Other personal devices

- ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes;

- enable and insist on the use of the school's internet connection only while on the school site;

- use their right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school internet connection where this is necessary.

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	✓						✓	
Non-communicative wearable tech (e.g. Fitbit)	✓				✓			
Taking photos on mobile phones				✓				✓
Taking photos on other camera devices (school iPads and cameras)	✓						✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails	✓							✓
Use of chat facilities, forums and closed groups in apps on school devices (e.g. whatsapp, facebook)				✓				
Use of social networking sites including live broadcasting			✓					✓
Use of school blogs	✓						✓	
Use of school Twitter account			✓					✓
Use of video broadcasting e.g. 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 incident flowchart to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of child abuse, the investigation will be referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content).

- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded.

- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.

- The school will manage Online Safety incidents in accordance with the School Behaviour Policy where appropriate.

- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police.

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Advisor or Local Authority Designated Officer (LADO).

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 Adviser Jane Weatherill *Via Somerset Direct where pupil involved* 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):

- 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;
- any site engaging in or encouraging illegal activity including radicalisation and terrorism;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- using school systems to run a private business;
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords);
- creating or propagating computer viruses or other harmful files;
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet.

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

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

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. Schools should populate the grid below marking appropriate possible sanctions.
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 / warning	Inform parents / carers	Refer to Headteacher	Further sanction e.g: Removal c network / internet access rights	Refer to technical support staff action re filtering / security etc	Refer to Police
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	✓			✓	✓	
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

Schools should populate the grid below marking appropriate possible sanctions.
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 may 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 Staff action re filtering etc	Warning	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			
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 to other staff		✓	✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners				L			
Breech of the school Online Safety policies in relation to communication with learners				L			
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils				L			
Actions which could compromise the staff member's professional standing	✓	✓	✓			✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓				✓	
Accidentally accessing offensive or pornographic material and failing to report the incident				L			
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise				L,P			
Breaching copyright or licensing regulations	✓	✓					
Continued infringements of the above, following previous warnings or sanctions							✓