eLIM School Online 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 Safety;
- work to empower the school community to use the internet as an essential tool for life-long learning.

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

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

The Online Safety policy approved by Governing body on: _____

Signature of Chair of Governors: _____

The next review date is: _____

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.

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.

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

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

Roles and responsibilities

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

The Online Safety Leader (School Business Manager) will work with the Headteacher who is also the designated Safeguarding Lead, 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, Safeguarding Lead, IT subject lead teacher, governor, IT technician and pupil's voice. Pupils are part of this group, to contribute their knowledge and use of technology.

Role	Responsibility
Governors	• Approve and review 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 • Ensure systems are in place that 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 to annually review Online Safety with the school's technical support
Online Safety Leader	• Lead the Online Safety working group • 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 • Attend updates 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 and sign the Staff AUP • Act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or concerns to the Online Safety Leader and check this has been recorded • Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum and respond • Model the safe and effective use of technology • Monitor ICT activity 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 sign the Pupil AUP and the agreed class internet rules • Participate in Online Safety activities, follow the AUP and report concerns for themselves or others • Understand that the Online Safety Policy covers actions out of school that are related to their membership of the school
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 • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any Online Safety issues that relate to the school • Maintain responsible standards when using social media to discuss school issues
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 through an enforced password protection policy • 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)

Education of pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to Online Safety'

School Inspection Handbook - Ofsted 2014

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 implementation of the Somerset ActiveBYTES scheme and the Online Safety progression that is part of the Somerset Primary Computing Curriculum.

Within this:

- key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset 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 extreme and commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology
- pupils will write and sign an AUP for their class [*which might be agreed class rules*] at the beginning of each school year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

Education and information for parents and carers

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

- providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates;
- raising awareness through activities planned by pupils;
- inviting parents to attend activities such as Online Safety week or other meetings as appropriate;
- providing and maintaining links to up to date information on the school website

Training of Staff and Governors

There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- the Online Safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the Online Safety Leader providing guidance and training as required to individuals and seeking LA support on issues
- staff and governors are made aware of the UK Safer Internet Centre helpline 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 behaviour.

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

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying e.g. telling a trusted adult or the Childline Phone number - 0800 1111.

Pupils, staff and parents and carers will be encouraged to report any incidents of online bullying and advised to keep electronic evidence.

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

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 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. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Prevent

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

Technical Infrastructure

The 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:
    - 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 IT subject leader
    - 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 (apart from possibly Foundation Stage and Key Stage One pupils) being provided with a username and password
    - 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 '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.
    - 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

- the internet feed will be controlled with regard to:
    - the school maintaining a managed filtering service provided by an educational provider that includes filtering of terms related to terrorism
    - the school monitoring internet use, being aware of the websites that are used and attempts to access inappropriate or illegal sites
    - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using a proforma
    - requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
    - 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 who will arrange for these to be dealt with immediately in accordance with the AUP

Data Protection

The schools Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

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
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- store or transfer data using approved services such as remote access, the Somerset Learning Platform (SLP), encryption and secure password protected devices
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection officer
- check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital and video images

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

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images both on school devices and personal devices where permission has been given by the Headteacher
- make sure that images or videos that include pupils will be selected carefully with their knowledge
- seek permission from parents or carers before images or videos of pupils are electronically published
- encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission
- help all parties to recognise that any published image could be reused and repurposed
- make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use
- publish a policy regarding the use of photographic images of children which outlines policies and procedures including disposal and deletion

Communication (including use of Social Media)

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

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that 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 safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this is required

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
- 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 Teaching Standards 2012
- staff are advised that no reference should be made to pupils, parents/carers or school staff
- advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- 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 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 that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Headteacher
- inform all that personal devices should be password protected
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- inform visitors of the school's expectations regarding the use 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

with respect to other personal devices

- ensure that staff understand that the AUP will apply to the use of their own portable device for school purposes
- enable and insist on the use of the school's internet connection while on the school site
- inform all that personal devices should be charged prior to bringing it to school
- maintain the 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

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 selecte staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		X	X					X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones or other camera devices			X					X
Use of personal devices		X						X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of messaging apps	X							X
Use of social networking sites	X							X
Use of blogs				X				X
Use of Twitter				X				X
Use of video broadcasting e.g. YouTube	X				X			

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.

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 computer. Neither the school nor Somerset County Council can accept liability for the material accessed, or any consequences resulting from internet use.

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

Reporting and Response to incidents

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

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- The Online Safety Leader will record all reported incidents and actions taken in the School Online Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log
- The designated Safeguarding Lead will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage Online Safety incidents in accordance with the School Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser 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 Safeguarding for Schools Adviser to communicate to other schools in Somerset. Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Safeguarding for Schools 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 (p 15):

- 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

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 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 Staff fc action re filtering etc
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		X			
Unauthorised downloading or uploading of files		X			
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		X			
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X		
Deliberate actions to breach data protection or network security rules			X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		X			
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		X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			
Using proxy sites or other means to subvert the school's filtering system			X		
Accidentally accessing offensive or pornographic material and failing to report the incident				L	
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise				L	
Breaching copyright or licensing regulations		X			
Continued infringements of the above, following previous warnings or sanctions		X	X		