Online Safety Policy

Mission Statement

We are a Church school and through our distinct Christian values we enrich the lives of our children and create an environment where there is opportunity to "Let Your Light Shine" (Mathew 5:16)

Our values are brought to life through our Love of Learning; our Faith; our Respect and our Partnerships.

Love of Learning - We provide an inclusive, meaningful, enjoyable curriculum to inspire and encourage pupils to reach their full potential. We nurture the social and emotional development of all our pupils and teach them how to stay safe and lead healthy lives. We develop their confidence and independence and encourage them to question and reason rationally.

Faith – We are proud to be a Church of England School. We promote the values and beliefs of the Christian faith whilst respecting and celebrating the beliefs and cultures of others.

Respect – We develop each child's sense of self-worth as well as their sense of responsibility. We encourage children to value diversity and the wonder of creation.

Partnerships – We work together with our families, the Church and the local and wider community, valuing their support.

HEADTEACHER: Mr Chris Burman

CHAIR OF GOVERNORS: Mrs Sue Owen

This policy is reviewed annually by the Local Governing Body (LGB).
Policy reviewed by the LGB February 2023
Please read in partnership with the Cyber Response Plan (on the school website)

CONTENTS

1 RATIONALE

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 the school's other policies. This Policy has been developed in consultation with representatives from all groups within the school. The Policy will be made available to parents/carers via the school website.

2 SCOPE OF THE POLICY

This Policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, Governors and community users) who have access to and are users of the School's ICT systems.

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, which may take place out of the 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/carers of known incidents of inappropriate online safety behaviour that take place in and out of the School.

The implementation of the online safety Policy will be monitored by the appointed Link Governor, meeting termly and reporting to the Governors.

The impact of the Policy will be monitored by the appointed Link Governor by looking at:

- Log of reported incidents.
- Internet monitoring log.
- Surveys or questionnaires of learners, staff, parents/carers.
- Other documents and resources.
- Future developments.
- The online safety Policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.

3 ROLES AND RESPONSIBILITIES

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the School community, though the day to day responsibility for online safety can be delegated.

An online safety Leader will be appointed who, working with the designated Child Protection Co-ordinator will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

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.
Headteacher and Senior Leaders	• Ensure that all staff receives suitable CPD to carry out their online safety roles. • Log, manage and inform others of online safety incidents. • Create a culture where staff and learners feel able to report incidents. • 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 Wessex Learning Trust 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 leader	• Maintain and inform the Senior Leadership Team of issues relating to filtering. • Ensure use of the network is regularly monitored in order that any misuse can be reported for investigation. • Inform others of online safety incidents. • Lead the establishment and review of online safety policies and documents. • 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 Wessex Learning Trust

Role	Responsibility
	• Meet with the designated safe-guarding leader to regularly discuss incidents and developments.
Teaching and Support Staff	• Participate in any training and awareness raising sessions. • Read, understand and sign the Staff Acceptable Use Protocol (AUP). • Act in accordance with the AUP and online safety Policy. • Report any suspected misuse or problems to the e-Safety Leader. • Monitor ICT activity in lessons, extracurricular and extended school activities.
Pupils	• To verbally acknowledge and follow the agreed class internet rules. • Participate in online safety activities, follow the AUP and report any suspected misuse. • Understand that the online safety Policy covers actions out of the School that are related to their membership of the School.
Parents/ Carers	• Endorse (by signature) the Pupil AUP. • Keep up to date with issues through newsletters and other opportunities.
Technical Support Provider	• Ensure the School's ICT infrastructure is as secure as possible. • Ensure users may only access the School network through an enforced password protection policy for those who access children's data. • Keep up to date with online safety technical information and update others as relevant- eLIM. • 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 the School's systems.

4 EDUCATION OF PUPILS

A progressive planned online safety education programme takes place through Computing and Jigsaw lessons and across the curriculum, for all children in all years, and is regularly revisited:

- Key online safety messages are reinforced through assemblies and at the start of each unit of work.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Pupils are guided to use age-appropriate search engines for research activities.
- Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff pre-check any searches.
- Pupils are taught to be critically aware of the content they access on-line and 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 will write and sign an AUP, which will be shared with parents/carers.

5 EDUCATION AND INFORMATION FOR PARENTS/CARERS

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

- Providing clear AUP guidance which they are asked to sign with their children and regular newsletter and web site updates.

6 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:

- There is a regular cycle of online safety training.
- All new staff receiving online safety training as part of their induction programme (via staff handbook and policy documents).

- The online safety Leader receiving regular updates through attendance at South West Grid for Learning (SWGfL), the LA and WLT and by reviewing regular online safety newsletters from the LA and WLT.
- This online safety Policy and its updates being shared and discussed in staff meetings.
- The online safety Leader providing guidance and training as required to individuals and seeking either LA and/or WLT support on issues.
- Staff and governors are made aware of where to find advice about safer Internet use.

7 CYBER-BULLYING

Cyber-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 behaviour:

- The school will follow procedures in place to support anyone in the School community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyber-bullying.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining the school's system logs, identifying and interviewing possible witnesses, and contacting the service provider and the Police.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber-bullying and the School's e-Safety ethos.
- Sanctions for those involved in cyber-bullying will follow those for other bullying incidents.

8 TECHNICAL INFRASTRUCTURE

The person(s) responsible for the school's technical support 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 the School's ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts

which might threaten the security of the School's systems and data with regard to:

- Downloading of executable files by users.
- 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 the school.
- Installing programs on the school's devices unless permission is given by the technical support provider or ICT co-ordinator.
- Use of removable media (e.g. memory sticks) by users on the school's devices.
- Installation of up-to-date virus software.

- Access to the school's network and internet will be controlled with regard to:
  - Users having clearly defined access rights to the school's ICT systems through group policies.
  - Users (apart from Foundation Stage and Key Stage One pupils) being provided with a username and password.
  - Users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details.
  - 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 teachers, visitors) onto the school's system. All "guests" must sign the staff AUP and are made aware of this online safety Policy.
  - Key Stage 1 pupils' access to the internet will be by adult demonstration with directly supervised 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 which will be adult directed.
- The internet feed will be controlled with regard to:
  - The school maintaining a managed filtering service provided by an educational provider.
  - The school monitoring internet use.
  - Requests from staff to use YouTube is acceptable, if carefully used and monitored.
  - Requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged.
  - Any filtering issues being reported immediately to eLIM or SWGfL helpline.
- The ICT System of the school will be monitored regarding:
  - The school's ICT technical support regularly monitoring and recording the activity of users on the school's ICT 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.

9 DATA PROTECTION

The SWGfL Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 2018.

The school will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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 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.

10 USE OF DIGITAL AND VIDEO IMAGES

Photographs and video taken within the school are used to support learning experiences across the curriculum, to share learning with parents/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.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils' full names will not be used anywhere on the school's website, particularly in association with photographs.
- Written permission from parents/carers will be obtained before images or videos of pupils are electronically published.
- 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.

11 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 all the school's business will use the School's official email service.
  - Ensure that any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) is professional in tone and content.
  - Make users aware that email communications may be monitored.
  - 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.
  - Ensure that personal information is not sent via email.
  - Only publish official staff email addresses.
- **With respect to social media:**
  - Control access to social media and social networking sites.
- **With respect to personal publishing:**
  - Teach pupils via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
  - Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of the school) and raise with their parents/carers, particularly when concerning pupils' underage use of sites.
  - Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction.
  - Outline safe and professional behaviour.
- **With respect to mobile phones:**
  - Allow staff to bring mobile phones into the school, but must only use them during break, lunchtimes or during non-contact when they are not in contact with pupils' unless they have the permission of the Headteacher.
  - Advise staff not to use their personal mobile phone to contact pupils, parents/carers.
  - Provide a school mobile phone for activities that require them.
  - Allow pupils to bring mobile phones into the school, but they must be kept in the school office while on the school's premises or during school hours.

12 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.

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, Somerset County Council nor Wessex Learning Trust 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.

13 REPORTING AND RESPONSE TO INCIDENTS

The school will follow Somerset County Council's flowcharts to respond to illegal and inappropriate incidents as listed in those publications:

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber bullying, illegal content etc).
- 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 Child Protection Co-ordinator will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with the school's procedures.
- The school will manage online safety incidents in accordance with the School Behaviour Policy where appropriate.
- The school will inform parents/carers of any incidents or concerns in accordance with the 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, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Safeguarding for Schools Adviser and eLIM 01823 356839 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 The Local Authority Designated Officer: 01823 358264 where pupil involved. Local Authority Designated Officer (LADO). The Local Authority Designated Officer: 01823 357823 where staff involved. The Police The LA Senior ICT adviser: 01823 356839 Jane Hutton at the Wessex Learning Trust

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 material.

14 SANCTIONS AND DISCIPLINARY PROCEEDINGS

Sanctions and disciplinary procedures will 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:

- 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.
- 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 the school's systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and 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.

Appendix 1

SAFE SEARCH ENGINES

We strongly recommend that parents consider which search engine they use by **default**. Existing safe search engines exist at:		
BBC Find	http://www.bbc.co.uk/cbbc/find/	A limited search engine aimed at KS1 learners.
SearchBox for Kids	http://www.searchbox.co.uk/kids.htm	A variety of safe search engines to allow choice.
Primary School Safe Search	http://primaryschoolict.com	A custom search engine powered by Google.
SWGfL Swiggle	http://www.swiggle.org.uk	A custom search engine powered by Google.
KidsClick	http://www.kidsclick.org/	Designed for kids by librarians.
Infant Encyclopaedia	http://www.parkfieldict.co.uk/infant/	Safe Independent Research for Infants.
Safe Search Kids	http://www.safesearchkids.com/	Based on Google SafeSearch.
KidRex	http://www.kidrex.org/	Based on Google SafeSearch.

Computers can be set to always open on these web pages using:
Tools>Internet options>Home Page.

Google Safe Search

Google has tools which will moderate the content. They call this safe search and the instructions for completing this task are at:
http://www.google.co.uk/familysafety/tools.html

What happens next

These search engines cannot guarantee that inappropriate content will not be received. Parents/carers should discuss with their children what will happen if their children view content that makes the child feel uncomfortable. This could include turning the monitor off and telling the parent/carer.