E-SAFETY POLICY

Author/Person Responsible	***Sarah Duncan***
Date of Ratification	***March 2021***
Review Group	***Standards Committee 1***
Ratification Group	***FGB***
Review Frequency	***Annually***
Review Date	***March 2022***
Previous Review Amendments/Notes	***New KCSIE guidance Sept 2020***
Related Policies	Allegations against staff; Behaviour; Code of Conduct; Complaints; Confidentiality; Educational Visits; Equality (including anti-bullying); Grievances; Health and Safety; Medical Needs (including intimate care); Positive Handling; Racist incidents; Recruitment; and Whistle-Blowing.
Chair of Governor's Signature	

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices:	E-Safety Policy	**DATE:**	04/03/21
EIA CARRIED OUT BY:	Kirsty Robson	**EIA APPROVED BY:**	Standards Committee 1

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for a positive impact
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		X
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)		X
Gender reassignment		X
Marriage and civil partnership		X
Pregnancy and maternity		X
Race		X
Religion and belief (practices of worship, religious or cultural observance, including non-belief)		X
Gender identity		X
Sexual orientation		x

Any adverse impacts are explored in a Full Impact Assessment.

St Michael's Church of England Primary School, Winterbourne

Learn ~ Care ~ Enjoy

This school aims to be a learning community in which all:

- Achieve their full potential
- Are motivated to work independently and collaboratively
- Take initiative and responsibility
- Show respect and consideration for others and their environment

This e-safety policy has been developed, and will be reviewed and monitoring by the following:

- Computing Subject Leader / PSHE Subject Leader
- Headteacher
- A governor representative
- Consultation with the whole school community has taken place through a staff meeting, Pupil forums, governors meeting, parents evening and the school website/newsletter.

Schedule for Development, Monitoring and Review

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Sean Tarpey – Safeguarding Andreas Burt – Technical Jo Briscombe – ICT Strategy Adviser

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity **(available via South Glos if needed)** and any network monitoring data from **Downend Secondary School's technical team**
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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, personal negative comments about staff members or making damaging comments about the school, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

The following sections outline the roles and responsibilities, policy statements and education in relation to e-safety for individuals and groups within the school.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the Computing Subject Leader. The designated person for child protection is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this policy.

- E-safety training is carried out annually for all staff alongside child protection training.
- An audit of the e-safety training needs of all staff is carried out annually.
- The Computing Subject Leader receives regular updates through attendance at SWGfL and LA training sessions and by reviewing regular e-safety updates from the local authority.
- This E-Safety policy and its updates shared and discussed in staff meetings.
- The Computing Subject Leader provides advice/guidance and training as required to individuals as required and seeks LA advice on issues where required.

Use of Social Networking Sites

All school staff should be aware when using social networking sites that anything said, shown or received could be made available to a wider audience than originally intended. They should follow and understand the following principles:

- Employees and individuals otherwise engaged by the school are not permitted to access social networking sites for personal use via school information systems or school equipment during school hours.
- They must not accept pupils/students as 'friends' and must not approach pupils/students to become their friends on social networking sites. Personal communication of this nature could be considered inappropriate and unprofessional, and make that individual vulnerable to allegations.
- Any student initiated communication, or on-line friend requests must be declined and reported to the Headteacher or designated school child protection colleague.
- Staff are advised not to be on line friends with ex or recent pupils of the school or other schools.
- They should not share any personal information with any pupil; including personal contact details, personal website addresses or social networking site details.
- If staff are on line 'friends' with any parent/carer linked with the school, they must ensure that they do not disclose any information or otherwise post details which may bring themselves, the school or their colleagues into disrepute. Staff must not engage in any on-line discussion about any child attending the school.
- School staff must not disclose, on any social networking site, any information that is confidential to the School, Governing Body, or Local Authority; or post anything that could potentially bring the School, Governing Body or Local Authority into disrepute.
- They must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the General Data Protection Regulation.
- Staff should not post photographs of pupils under any circumstances, and should not post photographs of colleagues or others in the school community without their express permission.
- Care should be taken to avoid using language which could be deemed as offensive to others.
- Staff are strongly advised to take steps to ensure their on-line personal data is not accessible to anybody they do not wish to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum.
- The expectation is that no child at the school will use any form of electronic communication to mistreat another member of the school, whether that be pupil or staff, and the school reserves the right to impose disciplinary sanctions on any child who does this. Parents are asked to discuss this aspect of the use of technology with their child at home. In the event of malicious accusations being made against any

member of the school community, the Headteacher may directly contact the social media service provider to report the incident and, in the event that the comment was hosted from an account known to be age restricted, request closure of that account. Further sanctions maybe evoked with reference to the Behaviour and Discipline Policy. Further action may be taken by informing the police if the action is in contravention of law.

- If the school is made aware of pupils using social media sites inappropriate to their age, the school will request that the social media service provider close the account due to the risk of safeguarding issues.

Breaches

While the Governing Body does not discourage school staff from using social networking sites, staff should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment.

The Headteacher may exercise his/her right to monitor the use of the School's information systems, including internet access, where it is believed unauthorised use may be taking place. If such monitoring detects the unauthorised use of social networking sites, disciplinary action may be taken.

If any instances or allegations of inappropriate use of social networking sites are brought to the attention of the Headteacher/Governing Body, disciplinary action may be taken.

The Governing Body reserves the right to take action to remove any content posted by school staff which may adversely affect the reputation of the school or the wider school community, or put it at risk of legal action.

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of students in e-safety is therefore an essential part of our school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- There is a planned e-safety programme (scheme of work) detailed below.
- Key e-safety messages are reinforced at least annually through an assembly and/or e-safety day.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems are discussed during the formation of class rules and reminded to the children during each computing lesson.
- Staff act as good role models in their own use of ICT.

Curriculum

E-safety is a focus in all relevant areas of the curriculum. The e-safety scheme of work **(part of the SG ICT scheme of work)** is linked to the Becta Signposts to Safety key e-safety elements of culture, contact, commerce and content. It identifies for each year group progression statements, learning outcomes, processes, skills and techniques, vocabulary, suggested software and web links, sample activities and assessment activities.

- **The CEOP approved 'Hector's World' will be used to teach younger children about e-safety and the SMART Crew for the older children.**

- In lessons where Internet Access is pre-planned, students 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.
- Where students are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Students are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Parents / Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this at least annually by:

- Providing clear Internet Access guidance
- Inviting parents to attend activities such as e-safety evenings

Technical Staff - Roles and Responsibilities

For **all** schools, the local authority provides technical guidance for e-safety issues, and the team are fully informed about the issues. Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

Secure passwords for the curriculum network are held by Downend School. This includes the wireless network 'key'. Individual staff passwords are encrypted and known only to the individual member of staff (they can be reset by Downend staff.)

The school ensures, when working with Downend School as our technical support provider, that the following guidelines are adhered to.

- School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and relevant Local Authority E-safety guidance.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Requests from staff for sites to be removed from the filtered list must be approved by the head teacher/ deputy head.
- In the event of the school technician needing to make requested changes to filtering, or for any user, this is carried out by a process that is agreed by the Headteacher.
- Any filtering issues are reported immediately to the Downend School technical team.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Internet Access Policy.
- Actual / potential e-safety incidents are documented and reported immediately to the Computing Subject Leader/ Headteacher who will arrange for these to be dealt with immediately. This can be done in person but must be followed up via email as soon as possible. It is important that the Headteacher is informed so the matter can be reported to governors. 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 systems and data.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up-to-date virus software.

- Personal data cannot be sent over the internet via e-mail or taken off the school site.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the Internet Access policy concerning the sharing, distribution and publication of those images. All images must be downloaded to the media drive and not stored on and deleted from personal cameras and devices.
- Staff ensure that pupils also act in accordance with their Internet Access policy.
- Student's work is only published on a public web site with the permission of the student and parents or carers.

Guidance on the Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the Internet Access policies.
- Students / pupils are taught about email safety issues through the scheme of work and implementation of the Internet Access policy.
- Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.

. The following table shows how the school currently considers these should be used.

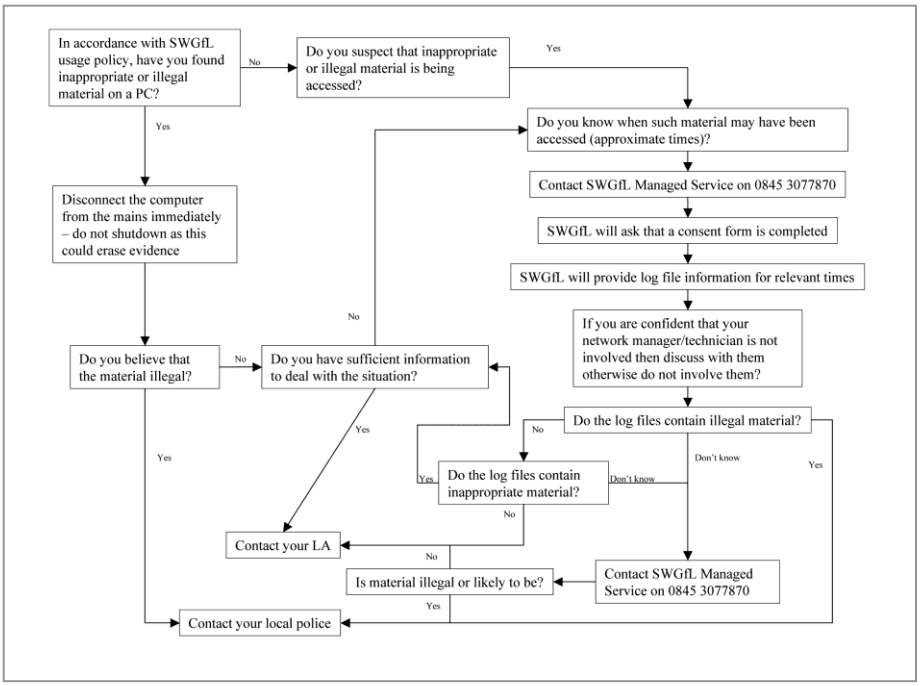
	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones			X					X
Use of hand held devices for personal use e.g. PDAs, PSPs				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 instant messaging				X				X
Use of social networking sites			X					X
Use of blogs		X				X		

Responding to incidents of misuse

We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse. If any apparent or actual misuse appears to involve illegal activity the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence. Illegal activity would include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials



If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not 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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling			X			
On-line shopping / commerce			X			
File sharing		X				
Use of social media				X		
Use of messaging apps					X	
Use of video broadcasting eg Youtube			X			

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy and Internet Access policies • E-Safety Governor works with the Computing Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	• Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. • Ensure that there is a system in place for monitoring e-safety • Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff • Inform the local authority about any serious e-safety issues including filtering • Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
Computing Leader:	• Lead the e-safety working group and dealing with day to day e-safety issues • Lead role in establishing / reviewing e-safety policies / documents, • Ensure all staff are aware of the procedures outlined in policies • Provide and/or brokering training and advice for staff, • Attend updates and liaising with the LA e-safety staff and technical staff, • Deal with and log e-safety incidents including changes to filtering, • Meet with E-Safety Governor regularly to discuss incidents • Report to Senior Leadership Team
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Internet Access policy • Act in accordance with the Internet Access and e-safety policy • Report any suspected misuse or problem to the E-Safety Co-ordinator • Monitor ICT activity in lessons, extra-curricular and extended school activities
Students / pupils	• Participate in e-safety activities, follow the Internet Access policy and report any suspected misuse • Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Annually endorse (by signature) the Student / Pupil Internet Access Policy • Ensure that their child / children follow Internet Access rules at home • Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school Internet Access Policy. • Keep up-to-date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data • Inform the head teacher/ computing leader of issues relating to the filtering applied by the Grid • Keep up to date with e-safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. • Ensure monitoring software / systems are implemented and updated • Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	• Sign and follow the Internet Access Policy before being provided with access to school systems.

Sample letter sent out to Parents and posted on website

Dear Parent/Carer

Social networking is used everywhere and is a common feature of many people's lives. However if you want to say anything about your child's school or staff on social media there are a few simple guidelines we need to insist you follow, in order to keep all the children in school **safe** and to protect you from possible consequences of your online actions. We already teach the children how to be safe online and you can reinforce this at home by showing your child(ren) how to communicate responsibly online.

Part of our role as a school is to ensure that no confidential information about a child or family is unintentionally disclosed by a parent/carer or a member of staff. There have been several high profile cases in the news when people making offensive comments on social media have been prosecuted.

There are two parts to this brief guidance. The first part is about parent/carer responsibilities. The second is information about what staff are expected to do if they use social media, or come across information about the school (children, parents or staff) on social media.

Guidelines for Parents and Carers

- At all times be respectful of others.
- Never include children's full names (even your own children's).
- Never post or tag photographs etc without ensuring that you have the right permission.
- If there is something you are concerned about in school please contact the school to sort it out rather than discussing it on Facebook for example.
- Everyone who adds to online sites is responsible for any comments posted under their name.
- If you are aware that sites are being misused you have a responsibility to report this.
- If an online conversation looks as if it might be derogatory you should not get involved in the discussion and refer the person to the school.
- You should not accept children as friends on a social networking site (many have the minimum age of 13).
- If you want to set up a site that refers to your child's school then please let the school know.
- If you are using social networking sites for school purposes remember that this is a school not personal area so personal comments should not be posted.
- Also if the site is representing the school then please make sure that the good name of the school is preserved and not brought into disrepute.

Staff and Volunteer Responsibilities

- No member of staff or volunteer is allowed to discuss any matter to do with pupils, staff or parents/carers through social media because of safeguarding requirements. This includes tagging photographs etc.
- Some members of staff or volunteers may have social network accounts as a parent or member of a local community group. They must not respond to any comments about the school they come across.
- Staff and volunteers are obliged to inform the school leadership of any concerns they have about comments being made by others.
- Staff have a duty to monitor online spaces and report anything of concern to the school leadership.

The school will always request that any inaccurate or offensive postings are removed. If necessary in an extreme case the school will take legal advice.

Thank you for your understanding and support.