Policy: Esafety Policy

Date: March 2017
Review date: March 2018
Authorised by: Governing Body
Updated by: Head Teacher

This e-Safety Policy has been developed, and will be reviewed and monitored, by our school e-safety working group which comprises:

- School eSafety Coordinator / ICT Subject Leader / PSHCE Subject Leader
- Headteacher
- A representative of teaching staff and support staff
- A governor representative and a parent representative

Consultation with the whole school community takes place through staff meetings, School Council meeting, governors' meeting, parents' evening and the school website/newsletter.

As a Church of England School we identify Christian values that underpin the whole of our community. These values inform our school's vision, aims and ethos, the design of our curriculum, all policies, planning and the school's management and governance. The values that relate particularly to this Policy are Service, Trust, Respect and Responsibility.

This Policy should be read in conjunction with our Acceptable Use Policy, Safeguarding (Child Protection) Policy, the Behaviour Policy and the Anti-Bullying Policy.

Schedule for Development, Monitoring and Review

This eSafety Policy was approved by the *Governing Body / Governors Curriculum Committee:*	March 2017
The implementation of this policy will be monitored by the:	eSafety working group
Monitoring will take place at regular intervals:	Annually during Term 3
The *Governing Body / Curriculum Committee* will receive a report on the implementation of this policy including reported incidents:	Annually during Term 6
This policy will be reviewed regularly and in the light of significant new developments or threats to e-safety.	Annually during Term 1
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Glos CC Safeguarding Contact: LADO: Jane Bee Technical Support at SWGfL Schools' Hardware Support Helpline at Glos CC – 01452 427205

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity and any network monitoring data from the LA 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 Head Teachers, 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, 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 Head Teacher 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 eSafety Leader.
The designated safeguarding lead 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.
Up to date guidance relating to training and e-safety matters can be found at www.swgfl.org.uk
Resources may be accessed with a specified username and password.

Staff and Governors
E-safety training is regularly planned for staff meetings, INSET and governors' meetings to ensure everyone understands their responsibilities, as outlined in this, and the acceptable use policy.

- An audit of the e-safety training needs of all staff is carried out annually
- All new staff receive e-safety training as part of their induction programme
- The E-Safety 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 E-Safety Leader provides advice/guidance and training as required to individuals as required and seeks LA advice on issues where required

Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of children 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 annually through an assembly and through e-safety week
- Children are helped to understand the student acceptable use policy and act accordingly
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children are taught about the risks associated with cyber-bullying
- Rules for use of ICT systems are posted in all rooms where ICT is used
- 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 identifies for each year group learning objectives, key skills, knowledge and understanding and suggested software and web links, with sample activities. The School takes part in Safer Internet weeks/days annually. Cyber-bullying is included in the Anti-Bullying Policy, and is included during the participation of Anti-Bullying week.

- In lessons where internet use is pre-planned, it is the responsibility of the staff to ensure that pupils are guided to sites checked as suitable for their use. Procedures are in place for dealing with any unsuitable material that is found in internet searches. Staff are responsible for pre-checking any searches.
- Where children 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 children to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Children are taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Children 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 by:
- Providing clear acceptable use policy guidance and regular newsletter and web site updates
- Providing an awareness raising meeting for parents

Technical Staff - Roles and Responsibilities
The Local Authority provides technical support, (Hardware Support Team) for the set-up and management of curriculum and admin servers. An independent technician is employed to manage day to day issues as they arise.

The school ensures, when working with 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.
- 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 and actioned by the head teacher and this is logged.
- In the event of the school technician needing to make requested changes to filtering, or for any user, this is logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues are reported immediately to the Hardware Support Team at Gloucestershire County Council.
- 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 Acceptable Use Policy.

- Actual/potential e-safety incidents are documented and reported immediately to the E-safety Leader who will arrange for these to be dealt with immediately in accordance with the acceptable use policy.
- 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.
- Within school the Administrator password is held by the ICT Subject Leader and the Technician. Hardware Support can access the system if necessary.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- The downloading of executable files by users may be restricted depending on the user profile.
- The installation of new programmes is overseen by the Technician and ICT Subject Leader.
- The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils' instant use of images that they have recorded themselves or downloaded from the internet. However, staff and 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 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 acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff ensure that pupils also act in accordance with their acceptable use policy.
- Children's work is only published on a public web site with the permission of the child 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 children as it provides an effective audit trail.
- Any digital communication between staff and children / 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 acceptable use policies.
- Children in Y5 and Y6 will have a whole class email address which is overseen by the class teacher. Children in Y3 and Y4 will have whole year group email addresses, overseen by the class teachers. A generic KS1 account is available for educational purposes, overseen by class teachers.
- Children are taught about email safety issues through the scheme of work and implementation of the acceptable use policy.
- Personal information is 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	✓							✓*
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices of images not involving children (Taking images of children may only happen on school memory cards – see Acceptable Use Policy)	✓						✓	
Taking photos on school trips Only using school memory cards	✓					✓**		
Use of hand held devices e.g. PDAs, PSPs	✓						✓	
Use a devices with internal cameras, eg Nintendo DS	✓							✓*
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails	✓							✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs		✓						✓

***** In exceptional cases a mobile phone may be brought in to school, where it will be placed in the School Office. At no time are children allowed to have mobile phones in school without the knowledge of a teacher.

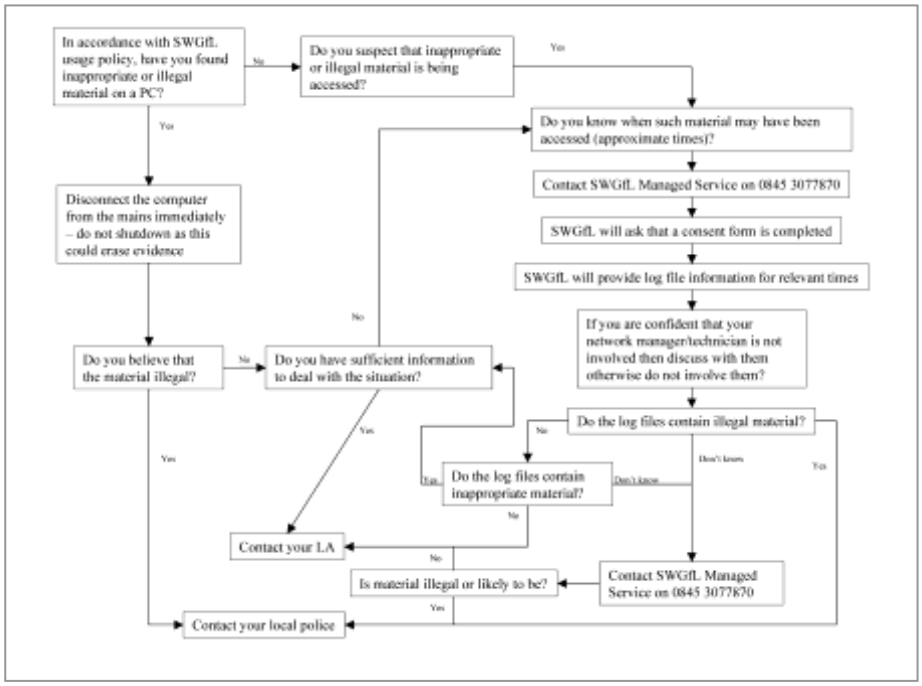
Where phones, or other devices with camera facility, are brought to school discos, or other after school events, in order to communicate to parents, the devices will be placed in safe storage until the end of the event.

** School trips: only school memory cards are allowed. Parents will not be able to use their own cameras or devices, and will be briefed accordingly.

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 school 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**					✓
	promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred					✓
	threatening behaviour, including promotion of physical violence or mental harm					✓
	any other information which may be offensive to colleagues, 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 SWGfL and / or 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 / personal, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line games (educational)		✓				
On-line games (non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce		✓				
File sharing (Blocked by SWGfL) **(Some sites that file share are places where spyware can access your files, computers and servers, personal/sensitive information might not be secure and there may also be copyright infringement issues.)**					✓	
Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users					✓	
Use of video broadcasting e.g. Youtube					✓	

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy & Acceptable Use Policies • E-Safety Governor works with the E-Safety 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.
E-Safety 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 to regularly to discuss incidents and review the log • Report regularly to Senior Leadership Team
Curriculum Leaders	• Ensure e-safety is reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Acceptable Use Agreement (AUP) • Act in accordance with the AUP 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 acceptable use 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	• Endorse (by signature) the Student / Pupil Acceptable Use Policy • Ensure that their child / children follow acceptable use 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 • Access to electronic messaging and payment systems • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure 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 of issues relating to the filtering applied by the SWGfL • 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 AUP before being provided with access to school systems.