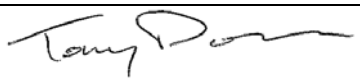
Brilliance, through Bowsland Best

E-Safety Policy

Author/Person Responsible	Computing Leader
Date of Ratification	15/06/17
Review Group	Computing Leader/Safeguarding Lead
Ratification Group	Children's Committee
Review Frequency	Annually
Review Date	June 18
Previous Review Amendments/Notes	January 2016
Related Policies	Safeguarding including Child Protection Acceptable Use Anti-bullying Any related curriculum policies
Chair of Governors Signature	

E-Safety Policy

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Children and young people should have an entitlement to safe internet access at all times. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

In their e-safety guidance (September 2012) Ofsted states that the breadth of e-safety issues can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

The purpose of this policy is to ensure that the school community are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this.
The policy also aims to protect children from radicalisation and provide guidance on what to do if they believe a child is being radicalised or groomed online.

1. Monitoring and Review

1.1 The policy is reviewed at least annually but also in response to new technologies being introduced or incidents that have taken place. The impact of the policy will be monitored using evidence from self-evaluation as identified below.

E-safety Self-evaluation

1.2 In order to understand the issues within our school community, we gather and use a range of evidence to inform development of our practice, planning for the curriculum and planned professional development. Self-evaluation is conducted through:

- Logs of reported incidents
- Network monitoring data from the LA technical team
- Surveys / questionnaires of pupils, parents / carers, and staff including non-teaching staff
- E-safety self-evaluation checklist and local authority safeguarding audit
- Pupil and parent views are regularly sought to inform developments

Our school uses the iBoss safe online tool as a filtering system for monitoring, producing reports which enable us to monitor children and staff behaviours online. This tool will be reviewed annually.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. It applies to systems in school and out of school where activities have been set by the school or are using school online systems.

2.1 The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils / 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.

2.2 This policy should be considered in conjunction with the following policies which it complements:

- Acceptable use policies for pupils, staff and parents / carers which outline acceptable behaviours when using technology
- Good Behaviour policy which outlines the procedures rewards and sanctions associated with online behaviour, including cyberbullying.
- Anti-bullying policy which details how issues of online bullying (cyberbullying) will be dealt with.
- Curriculum policy which outlines how ICT is used throughout the school

3. Roles and Responsibilities

3.1 Governors:

The children's committee are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the Safeguarding Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors committee and meetings

4. Headteacher and Senior Leaders:

- 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 will be delegated to the E-Safety Co-ordinator / Officer.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer. Additionally, reports from iBoss will be produced for the Senior Leadership Team to access.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents)

5. E-Safety Coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meeting / committee of Governors
- Reports to Senior Leadership Team

6. Network Manager / Technical staff:

South Glos and Computing leader are responsible for ensuring:
• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• That the school meets the e-safety technical requirements outlined in the computing policy and by iBoss cybersecurity

Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
• That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
• The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
• That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

• that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher for investigation / action / sanction

7. Teaching and Support Staff

Are responsible for ensuring that:
• They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
• They report any suspected misuse or problem to the E-Safety Co-ordinator / Headteacher investigation / action / sanction
• Digital communications with pupils / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
• E-safety issues are embedded in all aspects of the curriculum and other school activities
• Pupils / pupils understand and follow the school e-safety and acceptable use policy
• Pupils / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• They monitor ICT activity in lessons, extra-curricular and extended school activities
• They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
• In lessons where internet use is pre-planned pupils / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

8. Designated person for child protection / Child Protection Officer

Child protection officer will be informed of any 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
• cyber-bullying

9. Pupils / pupils:

• Are responsible for using the school ICT systems in accordance with the Pupil / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

10. Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:
• Endorsing as much as possible (by signature) the Pupil / Pupil Acceptable Use Policy
• Accessing the school website in accordance with the relevant school Acceptable Use Policy.

11. Education of Pupils and the Curriculum

11.1 Whilst regulation and technical solutions are important, their use must be balanced by educating learners to take a responsible approach. The education of pupils in e-safety is 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.

- We have an age-related e-safety curriculum that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, and how to take responsibility for their own and others safety and how to be responsible users of technology.
- E-safety is embedded in all relevant areas of the curriculum including research in History/Geography, publishing in English, social skills in PSHE, data handling in maths and core skills in ICT.
- The e-safety scheme of work identifies for each year group progression statements, learning outcomes, processes, skills, vocabulary, suggested software and web links, sample activities and assessment activities.
- Key e-safety messages are reinforced through assemblies.

- The Acceptable Use Policy is discussed with pupils in every class and all classes discuss their rules for e-safety which are displayed in classrooms and in the computer suite.
- Reference is made to E-safety in the Home-School Agreement for all parties.
- Pupils are given age appropriate support to search safely and to evaluate the content that they access online. Processes are in place for dealing with any unsuitable material that is found in internet searches. Staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Our Good Behaviour policy is also used to reinforce online behaviour with positive sanctions being used to reward positive and responsible use of ICT. Pupils also complete an e-safety award during Year 5.
- Older pupils are involved in providing support for younger ones through working on activities with them and presenting in assemblies.

- Staff use their teacher laptop to share with pupils how to deal with issues outside school where there may be no filtering
- Teachers monitor ICT use during lessons.

12. Use of Digital and Video Images

12.1 Digital imaging technologies create 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 / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm. Staff and pupils follow the clear guidance in the acceptable use policy concerning the sharing, distribution and publication of images.

12.2 Parents sign a consent form which allows photographs of their child to be used for publications, on twitter and on the web site. Photographs are carefully chosen and any published photographs or videos of pupils will not be used alongside full names.

13. Data Protection

13.1 The school comply with the 1998 Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant

- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

13.2 Staff ensure that they:

- Ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers / devices, ensuring that they are properly logged off at the end of a session using personal data
- Transfer data using encryption and secure password protected devices / memory sticks
- Delete personal data from portable devices once they have finished with it

14. Passwords

14.1 All users of ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. The youngest children in reception do not have their own password. Passwords for staff are regularly changed. Passwords are managed by the technical support provider and any changes are logged.

15. Filtering

15.1 Filtering is provided through iBoss cybersecurity service. This is monitored by the School Business Manager. Any changes to filtering are requested and managed through the South Gloucestershire IT helpdesk for all South Gloucestershire schools.

16. Use of Personal Equipment in School

16.1 Staff have use of school cameras and devices so use of personal devices images and video is not necessary or allowed.

16.2 Staff personal mobile phones or other devices should not be used to store contact details of parents and pupils.

17. Communications Technologies

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

17.2 The official school email service is used for communications between staff, and with parents/carers and pupils, as it is regarded as safe and secure, provides an effective audit trail and is monitored.

17.3 The acceptable use policies clearly outline how communication technologies, including e-mail, can be used to communicate across the school community and all sign up to these and follow them. The school ensures that, where

communication technologies are used then tools are chosen that enable staff to monitor their use.

18. Reporting and Dealing with Incidents

18.1 There are activities that are inappropriate in a school context and users should not engage in these activities in school or outside school when using school systems. These are detailed in Appendix 3.

18.2 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. School-based online reporting processes are clearly in place and understood by the whole school. They are detailed in the Acceptable Use Agreements and are summarised as follows:

- Pupils report any issue to their teacher or other adult
- Staff must immediately report any issue to the e-safety lead and, in the case of possible child protection issues, to the Head Teacher who is responsible for child protection
- Any issues that can not be resolved by the teacher are escalated to involve the Head Teacher
- The e-safety lead must report any issues to do with filtering to the local authority help desk. E-safety issues can also be escalated and should be reported to the following local authority staff.
  - Angela King – Safeguarding
  - Andreas Burt – Technical
  - Jo Briscombe – Teaching and Learning

- If any 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
- The e-safety lead is responsible for ensuring staff are kept fully informed about any issues and their resolution

18.3 Sanctions to be taken in cases of breach of the policies by staff / pupils are outlined in the Acceptable Use Policy.

18.4 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 assist those carrying out the investigation.

Appendix 1: Roles and Responsibilities

The following roles and responsibilities have been allocated and agreed across the school.

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and Acceptable Use Policies. Governors work with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering,
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 with the LA e-safety staff. Liaise with technical staff. Deal with and log e-safety incidents including changes to filtering. Meet with the Safeguarding Governor to regularly to monitor e-safety developments. 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.
Pupils / 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 Pupil / 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 / Merlin in accordance with the relevant school Acceptable Use 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 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 AUP before being provided with access to school systems.

Appendix 2 – Technical Support Provider Guidelines

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 South Glos 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 an individual username and password and are responsible for the security of their username and password.
- Where the local authority provides curriculum 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 and have an agreement in place for this.
- The school maintains and supports the managed filtering service.
- In the event of the school technician needing to make requested changes to filtering, including removing sites from the filtered list, this is logged and approved by the Head Teacher before being carried out. Any filtering issues are reported immediately to the South Gloucestershire 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 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.
- 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. This is done through secure file transfer or using encrypted memory sticks.
- There are a number of "supply" log ins that can be used to provide temporary access on to the school system for trainee teachers and visitors. These are allocated to

individuals and a log is kept of their use. Regular visitors / supply teachers have their own log in.

- Downloading of executable files can cause issues and compromise security and permission should be sought from the provider for this to happen.
- Staff are allowed to use their school laptop at home for planning purposes.
- Staff should not install any programmes on a school workstation / portable device without prior permission from the Head Teacher and advice sought from technical support.

Appendix 3 – Use of communication devices

	Pupils						
Communication Technologies	Allowed but kept off	Allowed at certain times	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 mobile phones			√				√
Use of school email for personal emails			√				√
Use of chat rooms/ facilities			√				√

Use of instant messaging			√				√
Use of social networking sites			√				√
Use of blogs		√				√`	