

Bromley Heath Infant School

Online Safety Policy

Author/Person Responsible	Jess Griffiths/Abigail Perry- Hodge
Date of Ratification	May 2026
Review Group	Curriculum Committee
Ratification Group	Curriculum Committee
Review Frequency	Annually
Review Date	May 2027
Related Policies	
Chair of Governor's Signature	
The Governing Body may from time to time review its Online Safety Policy and inform parents of any changes in writing. Signed _____ Curriculum Committee	

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices:	Online Safety Policy	DATE:	May 2026
EIA CARRIED OUT BY:	A Perry-Hodge	EIA APPROVED BY:	A Perry-Hodge

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)	No	N/A
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)	No	N/A
Gender reassignment (transsexual)	No	N/A
Marriage and civil partnership		N/A
Pregnancy and maternity		N/A
Racial groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers)		N/A
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		N/A
Sex (male, female)		N/A
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		N/A

This online safety policy has been developed, and will be reviewed and monitoring, by our school e-safety working group which comprises of:

- Computing Subject Leader
- Head Teacher
- Governors

Schedule for Development, Monitoring and Review

Policy ratified by the <i>Governing Body</i> on:::	
The implementation of this policy will be monitored by:	Governors
Monitoring will take place:	Annually
The <i>Governing Body</i> will receive a report on the implementation including reported incidents:	Annually
This policy will be reviewed:	Annually
Should serious e-safety incidents take place, the following external persons / agencies will be informed:	Nick Pearce Integra IT DPO Solutions for Schools Nicola Cook 01296 658502

Scope of the Policy

This policy applies to **all** members of the school community (including volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. It applies in school but also out of school where actions relate directly to school set activity or use of school online systems. This policy reflects existing legislation including the Educations and Inspections Act 2006 and the equslity Act 2010. Additionally, it also reflects the Education Act 2011, which 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 relevant 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. This policy should be read alongside the acceptable use policies for staff and pupils.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk: Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying. Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Keeping Children Safe in Education (KCSIE) 2025

Monitoring

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
 - parents and carers
 - staff.

Roles and Responsibilities

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

The Governing Board:

The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The Headteacher:

The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community. The head teacher is also the designated person for child protection and is responsible for:

- Ensuring that all staff understand this policy and that it is being implemented consistently throughout the school.
- Work with other staff, as necessary, to address any online safety issues or incidents
- Manage all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Providing regular reports on online safety in school to the governing body

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber bullying are dealt with appropriately in line with the school behaviour policy

Parents/Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Acceptable use:

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools, they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed. The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/reinforced through:

- Pupil acceptable use agreement
- Staff induction
- Staff handbook
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website
- Peer support
- Email updates
- Newsletter updates to families

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images ie., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences-harassment and stalking • Drug related offences • Weapons/firearms offences • Fraud and financial crime including money laundering N.B Schools should refer to guidance about dealing with self generated images/sexting-UKSIC Responding to and managing sexting incidents and UKCIS-Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating					

	computer viruses or other harmful files - Revealing or publicising confidential or proprietary information (eg. Financial/personal information, databases, computer/network access codes and passwords) - Disable/Impair/Disrupt network functionality through the use of computer/devices - Using penetration testing equipment (without relevant permission) NB. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber crime and harness their activity in positive ways-further information here					X
--	--	--	--	--	--	---

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (informed by the school's filtering practices and/or AUAs)			X	X	

unacceptable in school policies:	Promotion of any kind of discrimination				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				X	
	Infringe copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in the use of the internet)			x	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				x	

	Staff and other adults			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Communication Technologies		x		
Online gaming (educational)			x	
Online gaming (non-educational)				x
Online (educational) shopping/commerce		x		
File sharing		X		
Social media		X		
Messaging/chat		X		
Entertainment		X		

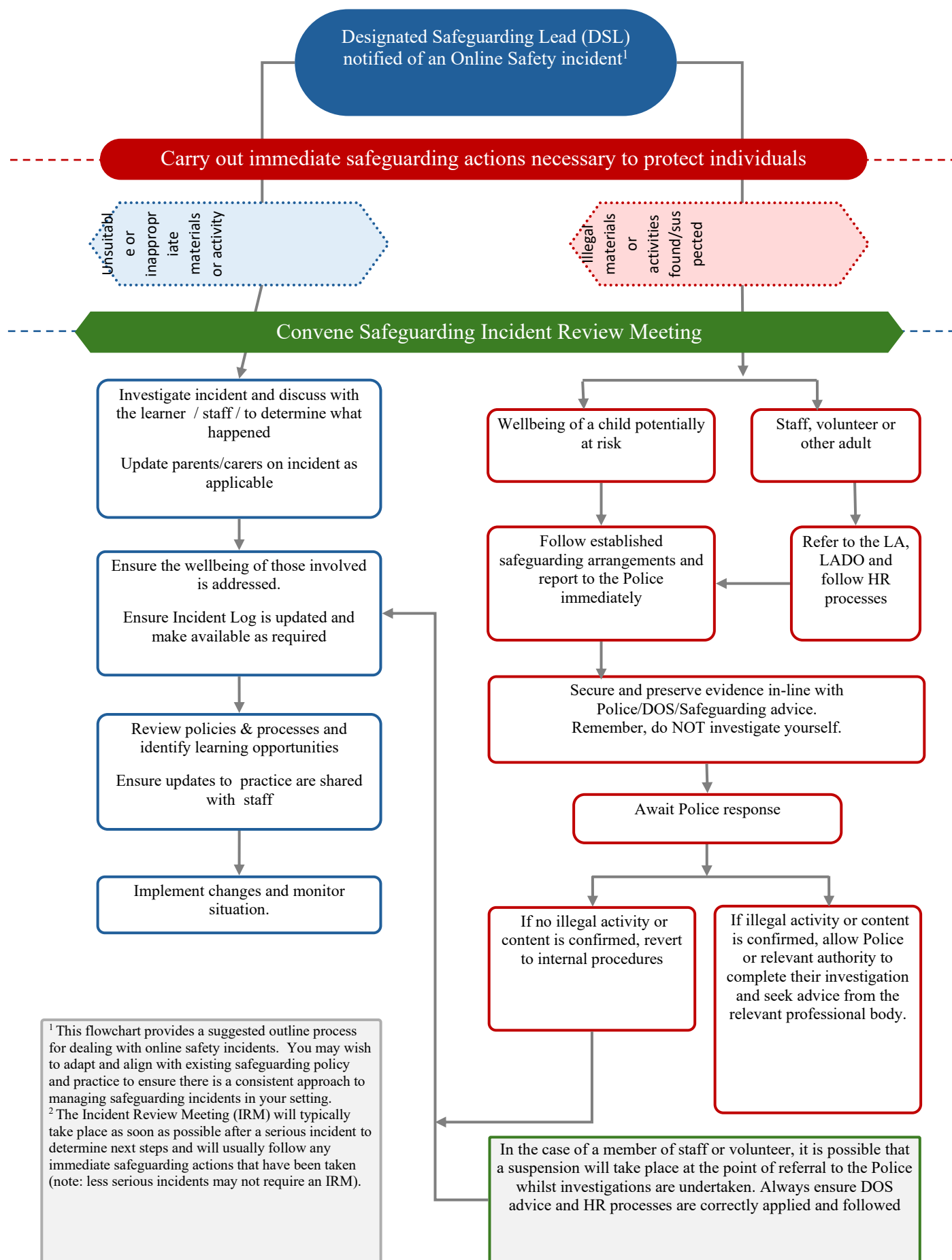
Streaming				
Use of video broadcasting		X		
Mobile phones may be brought to school	X			
Smart watches may be brought to school	x			
Smart watches used in lessons			X	
Use of mobile phones in lessons			X	
Use of mobile phones in social time	X			
Taking photos on personal mobile phones or other camera devices				X
Taking photos on school cameras	X			
Use of hand held devices eg PDAs				X
Use of personal email addresses in school, or on school network				x
Use of school email for personal emails				X
Use of messaging apps			X	
Use of wider social media				X
Use of blogs		X	x	
Use of X (Twitter)				
Staff publishing content (Youtube)		X		
Use of video conferencing (remote learning)		X		
Use of artificial intelligence with guidelines (as recommended by IT support)		x		

Mobile technologies

The use of personal devices or smart watches is prohibited for pupils in school (with exception for medical conditions).

Chart with acceptable use for staff + explanation that children cannot bring phones or smart watches to school.

The school will make the flowchart below available to staff to support the decision making process for dealing with online safety incidents:



Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Google Gemini or Microsoft Co-Pilot.

BHIS recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

BHIS will treat any use of AI to bully pupils in line with our behaviour and antibullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

Staff must not upload confidential, personal or safeguarding-sensitive information into generative AI platforms unless explicitly approved by the school and compliant with GDPR and data protection procedures. Any AI-generated content used for teaching or communication must be checked for accuracy and appropriateness.

Harmful online challenges and online hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

Cyber Security

[The DfE Cyber security standards for schools and colleges explains:](#)

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
 - impact on student outcomes
 - a significant data breach
 - significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
 - financial loss
 - reputational damage"
- Any hoax will be investigated using the incident flowchart, to identify, intervene in and escalate incidents where appropriate (in line with BHIS child protection, behaviour, staff behaviour or mobile device policies.)

[The 'Cyber-security in schools: questions for governing bodies and Trustees'](#) guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

[The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:](#)

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these

standards

- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner*), has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks:

-Hardware Snapshots - These snapshots are taken directly on the appliance that stores your data, once a day and kept for 30 days.

-Hyper-V Replication – Our file server is replicated to a 2nd datacentre every 15 minutes.

-Hardened Backup - The file server is backed up at the 2nd datacentre every day. The data in this backup cannot be deleted or edited while it is within retention and requires a dedicated highly-secured account to perform the modification. The minimum retention timeline is 14 daily backups, 5 weekly backups, and 6 monthly backups.

- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the BHIS's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework
- Lessons are matched to need; they are age related and build on prior learning
- Lessons are context relevant with agreed objectives leading to clear and evidenced outcomes

- Digital competency is planned and effectively threaded through the appropriate digital discussion in other curriculum areas
- Our curriculum incorporates/makes use of relevant national initiatives and opportunities e.g Safer Internet Day
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners 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
- Where learners are allowed to search the internet around a topic-they should use Swiggle (child search engine from SWGfL) or agreed websites signposted by the teacher. Staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- If particular websites or recommended apps are blocked by the filtering system, staff can request via the head teacher for this block to be removed by Integra IT, pending research of alternative approved apps and discussion with Integra IT.

Training and Awareness Raising

There is a planned programme of online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training sessions and by receiving regular online safety updates from the South Gloucestershire Traded Services.
- All staff, including support staff, receive an annual online safety update.
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The Online Safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.

Induction Processes

- All new staff receive online safety training as part of their induction programme.
- Parents of new reception children receive a briefing about online safety and processes when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.

Curriculum Provision

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum

should be broad, relevant and provide progression, with opportunities for creative activities. This will be planned and provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing lessons
- Key e-safety messages should be reinforced and regularly revisited as part of the Computing curriculum (the school has adapted the Kapow scheme to ensure this)
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Pupils should be guided to websites checked as suitable for their use; processes are in place for dealing with any unsuitable material that is found in internet searches
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

The following aspects also contribute to our curriculum provision:

- Coverage of the experiences is recorded and staff also check understanding when teaching about online safety.
- Opportunities to reinforce this are mapped to other subjects in the curriculum where appropriate for example: online behaviour is covered in PSHE.
- Assemblies are regularly used to reinforce online safety messages.
- Annual online safety events such as Safer Internet Day may also be used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils are helped to understand the school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Positive online behaviour is promoted through our scheme of work and is revisited annually.

Parents/Carers

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. The school will seek to provide information to parents and carers that children and young people can come across potential harmful and inappropriate material on the internet and may be unsure about how to respond. We will do this through:

- Curriculum activities
- Letters, newsletters, website
- High profile events eg. Safer Internet Day
- Communicating reported issues to parents so that they can take appropriate steps to follow these up with their child at home

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to improve online safety provision through the following:

- Local authority safeguarding audit
- Surveys with pupils and staff

Technical Issues

The local authority provides technical and curriculum guidance for online safety issues for **all** South Gloucestershire schools.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords and are encouraged to change these regularly. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in.** The same log in is used to access our governor online area, computing scheme of work and learner area. Access to systems is through groups so that only the relevant group of users can access a resource. Classroom computers/devices should always have the screen locked and password protected when being left unattended.

School owned/provided devices:

- Will be allocated to the year group using the Asset Register and regularly audited and checked by Integra IT and School Business Manager
- Personal use is not allowed as per the staff handbook
- Integra have full management of devices/installation of apps, changing of setting/Ios updates and monitoring
- Technical support provided by Integra IT
- Use on trips/events away from school is authorised for photos etc.
- Exit processes-devices returned if staff member leaves/checked at end of year/regular audit

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However, we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners.

Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged and documented by a process that is agreed by the Head Teacher. Any filtering requests for change and issues are reported immediately to the South Gloucestershire technical team on 3838.

Proactive monitoring is in place via a monitoring box provided by SWGfL. Should anyone attempt to access illegal content this is immediately reported to the police. Illegal activity would include attempting to access:

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**

- **other criminal conduct, activity or materials**

Virus Protection and Encryption

ESET Nod32 licences are obtained via INTEGRA; Anti-Virus daily updates also come via INTEGRA

Laptops at the school are encrypted by Integra as part of the bought in provision.

Connection to the network external is through secure VPN encrypted connection; also part of the SLA with Integra.

Technical Staff - Roles and Responsibilities

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.

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

- 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 and are provided with a username and password by the technical support provider.
- Users 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 and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- 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.
- 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.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that staff are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.

Use of Digital Images and Video

With the availability of mobile devices and tablets then taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff will 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 sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Parents sign permission forms to say that they will allow images to be taken of their child and used for educational purposes.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, newsletter or twitter feed. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the GDPR Act. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers as it provides an effective audit trail.
- 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.

Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site that governors can access to via a personal user account.

- Personal email addresses, text messaging, public chat and social networking programmes are not to be used for communications with parents/carers and children.
- The school uses Twitter to promote the school and update parents on news and events and this is managed and monitored by the computing subject leader.
- Guidance on personal use of social media and mobile devices is included in the acceptable use policy.

Copyright

The Head Teacher is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their:

- racial or ethnic origin,
- political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Transfer of Data

Whenever possible, secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear GDPR clauses in all contracts where personal data may be passed to third parties.
- The staff acceptable use policy clearly defines the GDPR measures that staff should take and how data can be securely stored and deleted.

Technical issues

The local authority provides technical and curriculum guidance for Online safety issues for all South Gloucestershire schools as well as providing direct technical support to a large number of schools.

Arbor provides technical support for the Management Information System

E-Limelight provides support for the school website.

Headteacher (as DSL) is able to manage content for Twitter.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all its users.

Internet access is filtered for all users by South Gloucestershire School IT. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

The strict filtering of content prevents children from accessing internet chat rooms or web pages where radical or terrorist extremist material is could be encountered. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.

However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that 'over blocking' does not restrict teaching.

Monitoring

The school recognises that filtering and monitoring systems are only one part of safeguarding and do not replace effective supervision, education and safeguarding procedures.

The school has monitoring systems in place to protect the school, systems and users:

- Integra IT Service Desk monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. Integra IT manage the monitoring system and alert the head teacher and online safety lead in instances of misuse.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising responses to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment which includes:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed

- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

The school reports issues through logging a call to the service desk at 3838 or emailing:

Servicedesk@integra.co.uk

Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838. Technical issues relating to Arbor (Information Management System) this will be managed by the School Business Manager, Headteacher or Online Safety Lead.

Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher.

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

- Online safety issues are reported to the Head Teacher. If these include allegations of bullying, then the anti-bullying policy is followed.
- Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed.
- Staff who are targeted by bullying online report these issues to the Head Teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.
- Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.
- If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (**Integra IT 01454 863838**).
- If access to an unsuitable site is reported, then the Online Safety lead will alert the technical support team by ringing **Integra IT on 01454 863838** to ensure that this is blocked.
- Serious incidents are escalated to local authority staff for advice and guidance
 - **Nick Pearce – IT & Infrastructure Services Manager– 863838**
 - **Jo Briscoombe – Curriculum and Policy – 863349**
 - **Jon Goddard – LADO allegations against staff and volunteers – 01454 868508**
 - **Linda Cordukes – Safeguarding and Child Protection - 5933**
 - **Arbor: Primary School Support – 020 8050 2086**
 - **E-Limelight (Website Provider / Host) – Clare Lester, 0117 214 0167**
www.elimelight.co.uk
- For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary **or 0344 381 4772**

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

There are defined sanctions in place for any breaches of the acceptable use policies. Suggestions for these can be accessed in [SWGfL policy template](#) (Word version with appendices) on pages 17 – 19. Schools are advised to adapt these to suit their own circumstances.

SWGfL provide clear guidance on what to do if there are suspicions that technology may be being mis-used in order to ensure that the right evidence is collected in a way that does not put the school at risk and these are followed. Refer to SWGfL policy template page 20.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and 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 on dealing with day to day e-safety issues (alongside class teachers/ the headteacher as necessary) 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, Report to Senior Leadership Team any concerns or updates
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 / 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.

This policy has been adopted by the staff and governors of BHIS and will be reviewed annually.

Signed: _____ Date: _____ May 2016_____

Review

Review date	May 16	Signed	√
Review date	May 17	Signed	√
Review date	May 18	Signed	√
Review date	May 19	Signed	√
Review date	Dec 20	Signed	√
Review Date	Dec 21	Signed	√
Review Date	May 2023 Amendments made re CSET/ Integra	Signed	√
Review Date	May 2024	Signed	√
Review Date	May 2025 Significant additions to include AI, Cyber Security and information on acceptable and unacceptable use	Signed	√
Review Date	May 2026 updated	Signed	√