Online Safety Policy

(Including Acceptable Usage Policies)

September 2025

Document control and record of amendments

Version	Reason for amendment	Sections amended	Amended by/date	Reviewed by/date	Approved by /date
1.0	New document	All	V Toppin June 2022		Governing Body 17.10.22
1.1	Annual update	All – typo's corrected, inclusion of visitor WiFi password, One-drive and Google services have been added, additional points in staff AUP (no.27 and edited no.24), pupil AUP added in iPads/school technology in the introduction	V Toppin June 2023	SLT June 2023	Staff September 2023
1.2	Annual update	Pages: 7, 9, 14, 15, 17, 19, 34, 37 Minor changes for clarity	V Toppin P Riddle September 2024	SLT September 2024	Staff & Governing Body 16th December 2024
1.3	Annual update	Pages: 8,10,16,18,19,21,23,30,31,34 Minor changes to reflect model policy and school practices	V Toppin P Riddle September 2025	SLT September 24	Staff & Governing Body 21.10.25

Date for Review: September 2026

Should serious online safety incidents take place, the following external persons/agencies should be informed:	Victoria Toppin (Online Safety Lead) Amanda Holliday (Co-Headteacher/DSL) Glen Tharia (Co-Headteacher) LADO Gloucestershire Police

Contents

Introduction

This policy applies to all members of the Elmbridge Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Computing Intent

Connecting with the future.
The Elmbridge curriculum allows pupils to develop the skills needed to communicate effectively, be creative and embrace ever-changing technology. We strive to enable pupils to become responsible digital citizens who engage with technology in order to enhance both their lives and the lives of others.

Links to Other Policies

Elmbridge Primary School will consider online safety when developing other policies, in particular:

- Accessibility
- Anti-Bullying, Equality and Hate incidents
- Attendance
- Behaviour and Relationships
- Children in Care
- Complaints
- Data Protection
- Drug Education
- Emotional Health and Wellbeing
- English as an Additional Language
- Intimate Care
- Medical Needs
- Offsite visits
- Pastoral Care
- Public Sector Equalities
- Pupil Premium
- Safeguarding and Child Protection
- Safer Recruitment
- Separated Parents
- Special Educational Needs Disabilities
- Spiritual, Moral, Social and Cultural Education (SMSC)
- Teaching and Learning
- Transition
- Wellbeing (including Relationships and Health Education)
- Whistleblowing
- Young Carers/Young Ambassadors

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. Andrea Stubbs of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures). This will follow the safeguarding policy.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and 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 online safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.
- Reporting to relevant Governors.
- Responsible for the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead for investigation/action/sanction.

Online Safety Lead

Victoria Toppin is our school Online Safety Lead. The Online Safety Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority (hardware support)
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Our ICT service is managed by Gloucestershire LA (hardware support). We have an ICT technician, Shelley Merrett, who works part time in school.
Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that monitoring software/systems are implemented and updated as agreed in school policies by SWGfL

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read and understood the staff acceptable use policy (AUP)
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Online Safety Team

The Online Safety Team is a group that has responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. This is group is made up of the Computing subject leaders, SLT, the safeguarding team who work alongside the ICT technician.
Members of the Computing Team will assist the Online Safety Lead with:

- the production/review/monitoring of the school online safety policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.

- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student/pupil records
- school-related messaging apps
- their children's personal devices in the school (where this is allowed)

Education

Pupils

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

At Elmbridge Primary School, as part of our Computing curriculum, each pupil will be taught age appropriate and progressive content in relation to online safety. Throughout each academic year, the children will cover the following topics:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, Wellbeing and Lifestyle
- Privacy and security
- Copyright and Ownership

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

- Key online safety messages will be reinforced as part of a planned programme of assemblies, for example 'Safer Internet Day'
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making.
- Pupils should be helped to understand the pupil acceptable use policy and be 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 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.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT technician can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through a variety of methods. These may include:

- Letters and newsletters
- Our school website
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced based on identified needs.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff may identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.

- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

At Elmbridge Primary School our internet provider is SWGfL, who manage our broadband connections; our main filtering and the ports that are open. We are also supported by Gloucestershire LA (hardware support), who manage the server. Our ICT technician manages the day to day support.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be reviews and audits of the safety and security of school technical systems every year.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the ICT technician must also be available to the Headteacher and senior leaders and kept in a secure place
- The ICT technician is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (for example, child sexual abuse images) is filtered by SWGfL by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- If filtering changes are required, requests are to be considered by the members of the Online Safety Team before authorisation. A decision log will be completed.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school use an active monitoring approach which alerts the online safety team to any potential safeguarding concerns.
- If there is a breach of security, users are expected to inform the Senior Leadership Team in a timely manner. The SLT will then contact either Gloucestershire LA (hardware support), The ICT technician or SWGfL.

- Appropriate security measures are in place (for example, server is password protected, SWGfL's firewalls and routers, wireless systems are password protected, work stations are password protected) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual devices are protected by up to date virus software.
- Supply and trainee teachers are given a generic user account. Visitors e.g. speakers during assembly, that require access to the network are logged on with school logins and are then supervised. Visitors that require WiFi access are given the visitor WiFi password.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download approved software and resources on school devices.
- Removable media (e.g. memory sticks/CDs/DVDs) can be used by users on school devices. These must be encrypted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The school recognises that the device then has access to the wider internet which may include the school's network and cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is part of the school's online safety education programme.
At Elmbridge Primary School, pupils are not allowed to use their own personal devices (phones, tablets, cellular smartwatches) in school. If a pupil needs to bring their device to school, it is be handed into the Hub before the start of the school day and can be collected as the pupil leaves the school site. These expectations are set out in the Pupil Acceptable Usage Policy.
Staff are permitted to use their own personal mobile phones and devices on the school site as set out in the Staff Acceptable Usage Policy.

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Stored in Hub	Yes	Yes
Full school network access (E.g. T-drive)	Yes	Yes	Yes	No	No	No
School Internet Only (Wifi)	Yes	Yes	Yes	No	Yes	Yes (visitor password)

School owned/provided devices:

- Staff are allocated devices as required, by SLT. For example, class teachers are given a work laptop, TAs have access to year group laptops. Students are provided 'personal' devices for lesson use by SLT and SENDCO based on individual needs.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Staff can use school owned devices in school and at home. Pupils can only use devices at school, unless remote learning when they can use the device at home.
- SLT, the safeguarding team, SENDCOs, the ICT technician and admin staff have access to the G-drive; other staff have access to the T-drive/E-drive (cloud based). Staff will be able to access the school One Drive storage through their Microsoft Office 365 log in, with two-factor authentication. When in school, pupils have access to the P and R-drives but when working from home cannot access the school network.
- The ICT technician and SLT can download apps/programmes onto other devices.
- When working in school, devices will connect to the school network (within permissions) and when working from home devices will need to connect to the users own internet service.
- Devices are supported by the ICT technician.
- When onsite, school devices are filtered by SWGfL. When devices are used at home, filtering is carried out by the home provider. The virus software can identify sites visited and is monitored by the ICT technician.
- As a school, we use online Google services, including Google drive. The accounts are created/deleted as necessary.
- Photos can be taken on school devices.
- When a member of staff leaves, the devices are left in school, recalibrated and reissued where needed.

Personal devices:

- Staff may use their own personal devices in school.
- Staff devices are their own responsibility.
- Staff are encouraged to keep their personal possessions in a safe place.
- Staff should only use personal devices when not in charge of pupils unless they have permission from SLT. For example, if using as a teaching aid. Staff should have mobile phones on silent/vibrate during lesson times but may use if being contacted by a staff member for an immediate need eg a phone call from office to a collection of a child.
- Staff can use their personal devices for school business. Staff are advised to block their number, but this is left to staff discretion.
- Staff are encouraged (where possible) to use the school WiFi whilst on site.
- Staff should not use their personal devices for taking photos of school based activities without the express permission from the SLT.
- Pupils are to hand in their personal devices to the Hub before they enter the playground at the start of the day and can collect as they leave the site at the end of the day. Parents are expected to complete a 'consent form for mobile phones to be kept in school'.
- Visitors can keep their devices in their possession. They must follow the school's safeguarding procedures.

- Visitors will be given our visitor booklet on arrival. For large groups of visitors, announcements are made.
- Personal devices do not connect to the school network, unless authorised by SLT for work purposes.
- Technical support is offered for personal devices, where devices are needed for purposes of 2FA.
- If personal devices are connected to the WiFi, SWGfL filtering applies.

Use of digital and video images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local media.
- 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 such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. Parents will be reminded of this during events where images may be taken.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment; the personal equipment of staff should not be used for such purposes without the permission of the Senior Leadership Team.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used on the school website, particularly in association with photographs.
- Digital images, that are no longer required, should be deleted by the end of each academic year, including those on ipads.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with professionals/parents/carers about a school matter.
- Users must immediately report, to the Headteacher – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff, professionals or parents/carers must be professional in tone and content.
- Whole class email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted Inspection Framework (safeguarding) reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise.
Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.
All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online

bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers, school staff or the school setting
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites outside of school teaching hours

Monitoring Public Social Media:

- If the school is made aware of negative or harmful social media comments made by others, the school will respond effectively.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

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 i.e., 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					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					X

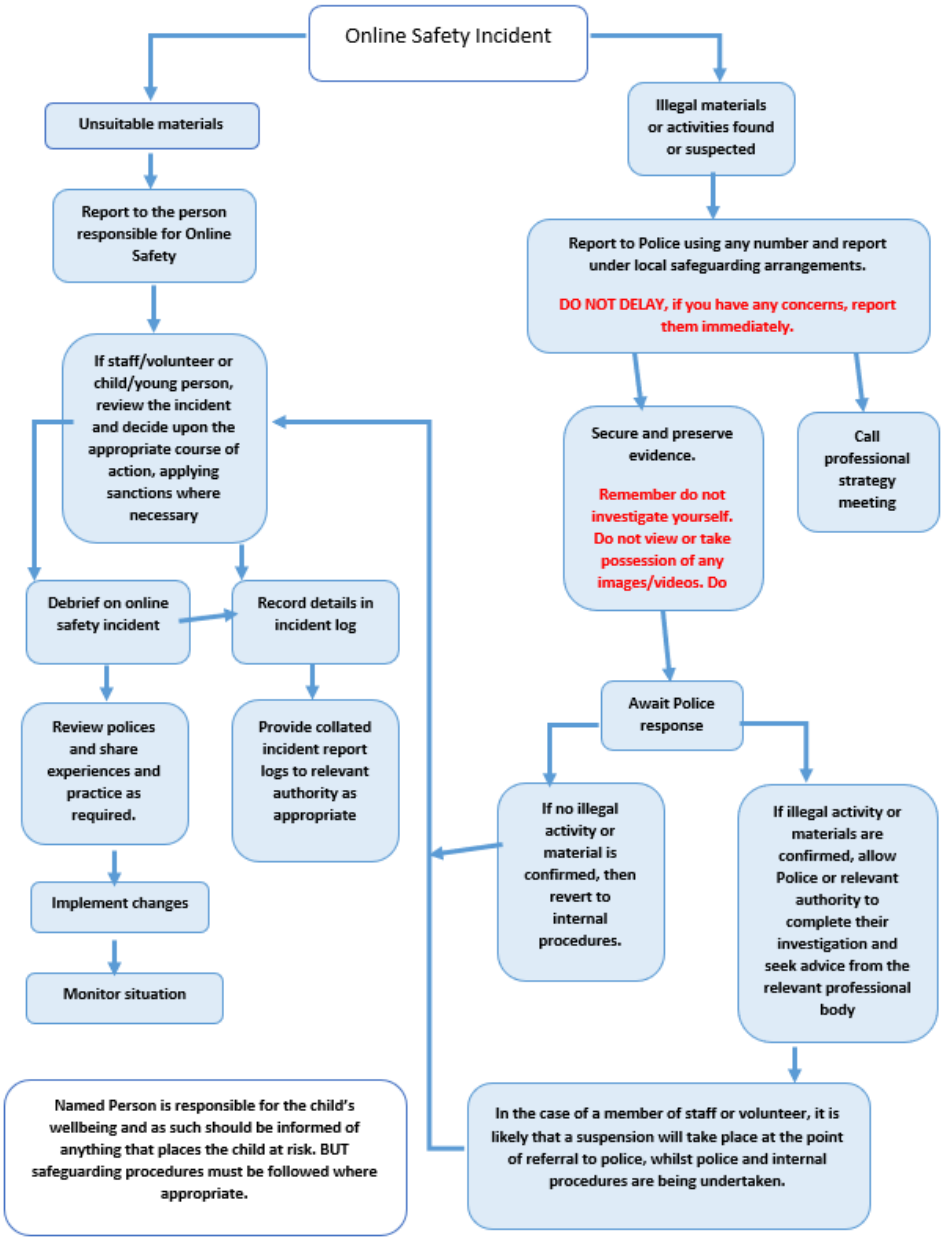
User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUPs)			X	X	
	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/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their 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	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions and sanctions

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Students/Pupils Incidents	Actions/Sanctions					
	Refer to class teacher	Refer to Head of Year/Online Safety	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X				X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X			X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X				X
Unauthorised downloading or uploading of files	X	X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X			X	X

Attempting to access or accessing the school network, using another student's/pupil's account	X	X			X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X
Corrupting or destroying the data of other users	X	X			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X

Continued infringements of the above, following previous warnings or sanctions may result in suspension or exclusion.

Staff Incidents	Actions/Sanctions				
	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	
Inappropriate personal use of the internet/social media/personal email	X	X			
Unauthorised downloading or uploading of files	X	X			X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			
Deliberate actions to breach data protection or network security rules	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	X	X	X		
Actions which could compromise the staff member's professional standing	X	X			

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X
Breaching copyright or licensing regulations	X	X			X

Continued infringements of the above, following previous warnings or sanctions may result in disciplinary action.

Appendix 1 – Staff Acceptable Usage Policy

School networked resources, including SIMS, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council/Local Authority, you must state that it is an expression of your own personal view. Any use of the network that may bring the name of the school or County Council/Local Authority into disrepute is not allowed.

Users are expected to utilise the network systems in a responsible manner. Computer systems may be monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with (see also Keeping Children Safe in Education). If anyone is aware of any breach of this policy, they should refer to the Online Safety and Safeguarding policies.

1	Do not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or Gloucestershire County Council) into disrepute.
2	Use of the school's computer systems for any kind of illegal activity, either directly or indirectly (for example by forwarding illegal material into/out of the school systems) is strictly forbidden.
3	Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group. Use appropriate language – remember that you are a representative of the school on a global public system.
4	SLT will monitor staff key stokes on any device that uses their school login. Staff under suspicion of misuse will be placed under retrospective investigation or have their usage monitored further.
5	Privacy – Do not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person. Do not reveal any personal information to students.
6	Do not trespass into other users' files or folders without consent.
7	Login credentials (including passwords) are not to be shared with any other individual, displayed or used by any individual other than yourself. Likewise, do not share those of other users.
8	If you think someone has learnt your password then change it immediately to a secure password (10 characters or more, include a variety of upper/lowercase letters, numbers and symbols)
9	Staff must only use USB drives (memory sticks)/portable devices that are encrypted.
10	After network sessions are finished, ensure you log off.

11	Do not use personal digital cameras, iPads or camera phones for creating or transferring images of children and young people without the expressed permission of the school leadership team.
12	E-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	Do not use the network in any way that would disrupt use of the network by others.
14	Report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the Headteacher.
15	Do not attempt to visit websites that might be considered inappropriate or illegal. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	Do not download any unapproved software, system utilities or resources from the internet that might compromise the network or are not adequately licensed.
17	Do not accept invitations from pupils to 'add me as a friend' to their social networking sites, nor invite them to be friends on yours. Do not contact pupils directly via email or social networks. Damage to professional reputations can inadvertently be caused by quite innocent postings or images. Be careful with who has access to your pages through friends and friends of friends (especially with those connected with professional duties, such as school parents and their children).
18	Ensure that any private social networking sites / blogs etc. created, or actively contributed to, are not confused with your professional role in any way.
19	Support and promote the school's Online Safety and Data Protection policies and help students be safe and responsible in their use of the internet and related technologies.
20	Do not send or publish material that violates the Data Protection Act or breaches the security this act requires for personal data, including data held on SIMS.
21	Do not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
22	Do not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
23	Ensure that portable ICT equipment such as laptops, iPads, digital still and video cameras are securely stored away when they are not being used.
24	Ensure that any personal data (where the Data Protection Act applies) sent over the internet will be encrypted or otherwise secured. E.g. through Egress. This should only be done through the school issued email address.
25	Teacher iPads **must** be password protected. Pupil images taken using portable devices such as iPads must only be published within the school's domain e.g. on the website and with the permission of the child's parents. No images are to be transferred over the internet and must be deleted from Teacher iPads at the end of each term. Pupil iPads are not to be taken off-site unless they are password protected.

26	Staff phones can log onto the WIFI and use this to access email or the internet if required. Staff may need to use 3G/4G/5G network if some sites are filtered, particularly in relation to safeguarding. Therefore, the school does not require staff to disable mobile data on their own devices, but to use their device in accordance with these rules.
27	Staff must not open emails from senders that they do not recognise and must report any suspicious emails to the Headteacher.
28	School allows unofficial communication between staff using WhatsApp. Staff must ensure that no pupil/parent data is shared in these groups. The tone of these groups must remain professional. Enrolment in these groups is not compulsory.

Additional guidelines

Staff must comply with the Acceptable Use Policy of any other networks that they access in any other educational settings.

Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or personal errors or omissions. Use of any information obtained via the network is at one's own risk.

Network security

Users are expected to inform the head teacher immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network may be regularly checked by the head teacher.

Media publications

Written permission from parents or carers must be obtained before photographs of named or unnamed students are published.

This policy extends as far as practicable to cover use of school/non-school technology to support remote learning but further arrangements may need to be considered dependent on the specific nature of remote learning (for example relaxation of security arrangements for use of private (non-school) internet connections when home learning is in place.

Remote learning (Para 138 of KCSIE September 2025)
Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at:
Safeguarding and remote education - GOV.UK

The NSPCC also provide helpful advice – Undertaking remote teaching safely.

Signed:…… Date: ……

Appendix 2 – Pupil Computer Acceptable Use Policy

EYFS and Key Stage 1

All children must follow the rules for using technology in school. If any rule is broken there will be a consequence. Teachers will show pupils how to use the computers and iPads.

1	I will ask permission before using the internet and will not access social networks or YouTube without permission
2	I will only use polite and sensible words when sending messages.
3	I will be supervised when using school technology.
4	I must not tell anyone over the internet: my name, where I live, my telephone number or my school or arrange to meet them.
5	I must not tell my private username and passwords to anyone.
6	I must never use other people's usernames and passwords.
7	If I think someone knows my password then I will tell my teacher.
8	I must log off after I have finished with my computer.
9	I will report any websites or messages that make me feel worried to an adult.
10	I will treat equipment and other's work with respect.
11	If I see anything that I am not happy with, I will tell an adult straight away and not show it to other children.
12	I will put equipment away carefully.
13	I will not bring in technology from home to use in school. If I need to do so then it will be put in the Hub until the end of the school day.

Key Stage 2

All children must follow the rules for using technology in school. If any rule is broken there will be a consequence. Teachers will show pupils how to use the school technology.

1	I will only use polite language when using the computers.
2	I must not write anything that might upset someone or give the school a bad name.
3	I know that my teacher will regularly check what I have done on the school computers and school-based websites.
4	I know that if my teacher thinks I may have been breaking the rules they will check on my previous use of the computers.
5	I must not tell anyone over the Internet, my name, where I live, my telephone number or my school and I will not arrange to meet them.
6	I must not tell my private username and passwords to anyone.
7	I must never use other people's usernames and passwords or computers left logged in by others.
8	If I think someone has learned my password then I will tell an adult.
9	I must log off after I have finished with my computer.
10	I must not use the technology in any way that stops other people using them.
11	I will report any websites that make me feel uncomfortable to an adult.
12	I will tell an adult straight away if I am sent any messages that make me feel uncomfortable.
13	I will treat equipment and other's work with respect.
14	If I find something that I think I should not be able to see, I must tell an adult straight away and not show it to other pupils.
15	I will not use social networks or YouTube in school unless my teacher has given me permission and I am old enough to do so. For example, children should be aged 13 and over to use Facebook/Snapchat and over 13 to use WhatsApp.
16	I ensure that portable ICT equipment such as laptops, iPads, digital still and video cameras are securely stored away when they are not being used.
17	I will not bring in technology from home to use in school. If I need to do so then it will be secured in the Hub until the end of the school day.

Acknowledgements

Elmbridge Primary have based this policy on the SWGfL model policy.
SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.