Evergreen Primary School
Online Safety Policy

Contents

Evergreen Primary School
Online Safety Policy

Introduction

Our policy uses the SWGfL template

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety in addition to its commitment to provide educational establishments in the South West of England with safe, secure and reliable broadband internet connections and broadband-enabled teaching & learning resources and services.

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk/

SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa. More information about its wide ranging Online Safety services for schools can be found on the SWGfL website – www.swgfl.org.uk

This policy should be read in cconjunction with the schools policy for Child Protection and Safeguarding, Keeping children Safe in Education 2016 and the schools Equalities Policy

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of

- Head of School
- Online Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	Summer Term 2017
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator and Senior Leadership Team
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Termly Governor Committee Meetings
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	Summer Term 2018
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, First Contact, Police

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires and discussions with
  - students / pupils
  - parents / carers
  - staff
- Discussions at parent meetings and Annual Review Meetings

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school , but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated safeguarding and child protection policy, behaviour policy and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

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 School Committee receiving regular information about Online Safety incidents and monitoring reports. A member 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 Co-ordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings and liaising with Link Governor

Executive Headteacher and Senior Leaders:
- The Executive 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 Co-ordinator

- The Executive Headteacher and Head of School 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 "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures.

- The Executive Headteacher and Head of School are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant. SWGfL BOOST includes access to unlimited online webinar training – further details are at http://www.swgfl.org.uk/Staying-Safe/Online Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development

- The Executive Headteacher and Head of School 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:
It is strongly recommended that each school should have a named member of staff with a day to day responsibility for Online Safety. Deborah Scurr is the Online safety officer at Evergreen And she is supported by Judith Benson – Head of School- and designated Safeguarding Lead. Their role is to

- take day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school technical staff
- receive reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governor meetings
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:
The School Technician – Gavin Thompson is 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, in which passwords are regularly changed
- 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 the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Executive Headteacher / Head of School / Online Safety Coordinator for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school

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, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Head of School /Online Safety Coordinator/ Executive Headteacher for investigation / action / sanction

- **all digital communications with pupils / parents / carers should be on a professional level** and only carried out using official school systems via Durham email
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety 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 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

Child Protection / Safeguarding Designated Person

The DSL is 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 on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator 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 / incident logs
- consulting stakeholders – including parents / carers and the pupils about the Online Safety provision
- monitoring improvement actions identified

E Safety Group
Judith Benson
Deborah Scurr

Evergreen Primary School
Online Safety Policy

Gavin Thompson
Governor / Parent
Members of the School Council

Students / 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 cyber-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 / VLE 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 / VLE and on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed)

Community Users
Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

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.

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 is provided as part of Computing / PHSE / other lessons and should be regularly revisited

- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line 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 helped to understand the need for the pupil 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 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, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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.

Education – 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 on-line 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:
- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community
The school may, where appropriate, provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:
- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide Online Safety information for the wider community
- Supporting community groups to enhance their Online Safety provision.

Education & Training – 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. An audit of the Online Safety training needs of all staff will be carried out as part of the induction process. It is expected that some staff will identify Online Safety as a training need within the performance management process.
- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator and DSL will receive regular updates through attendance at external training events from 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 / briefings/ INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required. SWGfL BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff (http://www.swgfl.org.uk/Staying-Safe/Online Safety-BOOST/Boost-landing-page/Boost-Hub/Resources). It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / Online Safety / health and safety / child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

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 regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.
- Where appropriate to their cognitive ability users will be provided with a username and secure password by Gavin Thompson who will keep an up to date record of

users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.

• The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Executive Headteacher and Head of School and kept securely in the school safe.

• Gavin Thompson Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband / filtering provider **Lightspeed Filtering Systems** actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Requests should be made to Judith Benson.

• The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for staff / pupils.

• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

• An appropriate system is in place, E Safety Incident Sheet, for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. See appendix

• Appropriate security measures are in place 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. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

• An agreed policy is in place for the provision of temporary access of "guests" eg trainee teachers, supply teachers onto the school systems.

• An agreed policy is in place AUP 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 AUP that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.

• An agreed policy is in place in the Data protection policy regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

Bring Your Own Device (BYOD)
Pupil use of own devices in school is not allowed except in extenuating circumstances for example a pupil may have an iPad on transport as a behavior support. These devices will be kept safe by an adult whilst the pupil is in school and should not be used whilst in school.

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 cyberbullying 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.
- To respect everyone's privacy and in some cases protection Parents / carers are asked not to take videos and digital images of their children at school events where other pupils are included.
- Staff 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 only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- 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 in accordance with parents/cares permission and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website. Class staff should ensure they are aware of permissions for pupils in their class.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- 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
- Only transferred to others with adequate protection.

The school must ensure that:
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

- It has a Data Protection Policy (Staff drive – policies folder)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Coordinator (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- 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 Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly **"logged-off"** at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:
- the data/device must be encrypted and/or password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete.

Communications

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		*						*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time		*						*
Taking photos on mobile phones / personal cameras				*				*
Use of other mobile devices eg tablets, gaming devices		*					*	
Use of personal email addresses in school, or on school network				*				*
Use of school email DLG for personal emails				*				*
Use of messaging apps		*						*
Use of social media				*				*
Use of blogs			*					*

When using communication technologies the school considers the following as good practice:
- The official school email service, DLG, 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 DLG school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the Executive Head Teacher or Head of School – 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 and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems - DLG. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils, where appropriate will be provided with individual school DLG 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

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- • Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- • Clear reporting guidance, including responsibilities, procedures and sanctions
- • Risk assessment, including legal risk

School staff should ensure that:

- • No reference should be made in social media to pupils, parents / carers or school staff
- • 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.

The school's use of social media for professional purposes will be checked regularly by the SLT and Online Safety coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 / academy 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

Evergreen Primary School
Online Safety Policy

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)			X			
On-line gambling					X	

|					
On-line shopping / commerce – ordering resources			X		
File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting eg Youtube			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 (see "User Actions" above).
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 (below and appendix) for responding to online safety incidents and report immediately to the police.

Evergreen Primary School
Online Safety Policy
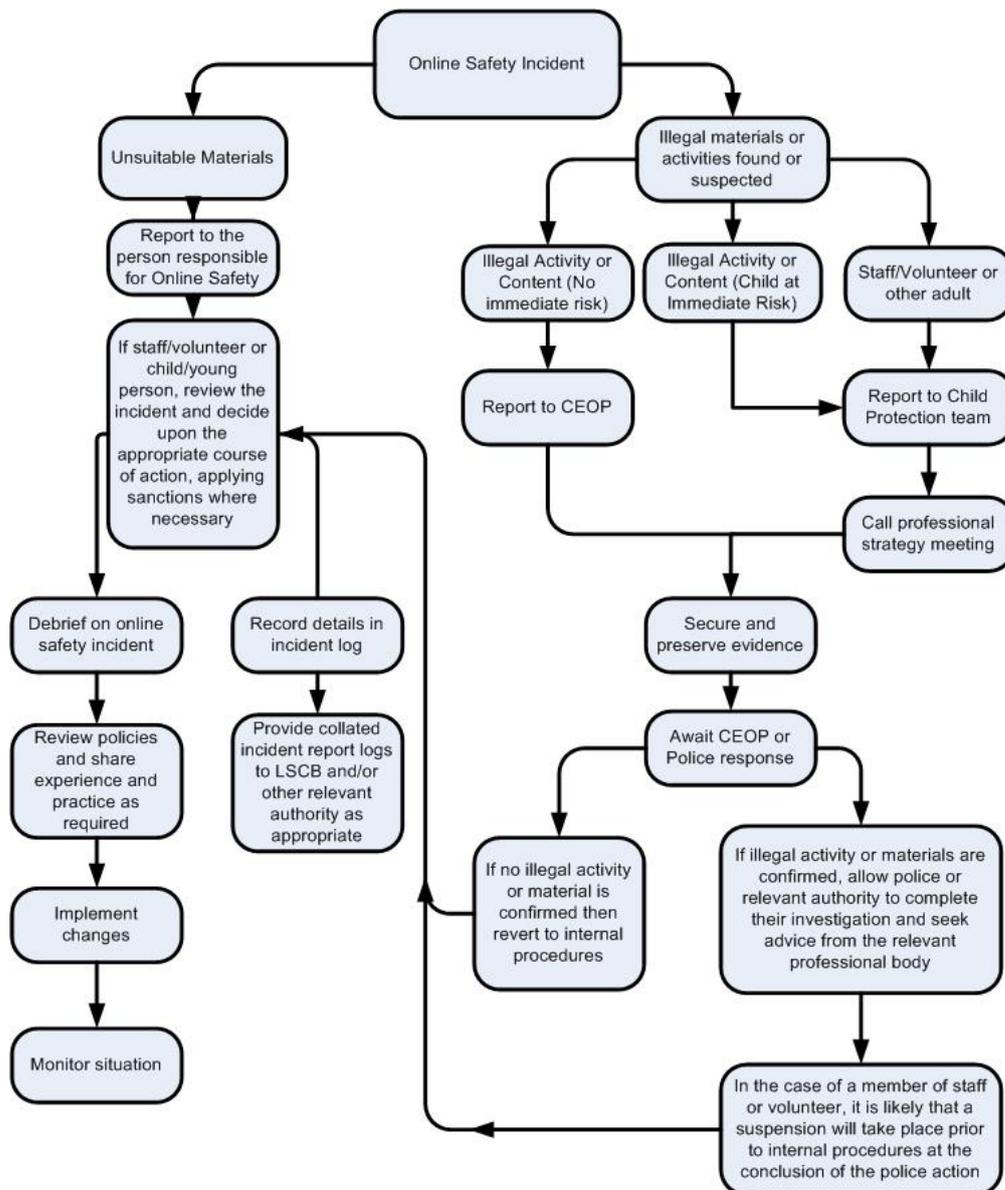
Other Incidents

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
  - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & 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:

Evergreen Primary School
Online Safety Policy

Pupils   **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to E Safety Co-ordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents /	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	X
Unauthorised use of social media / messaging apps / personal email	X	X							
Unauthorised downloading or uploading of files	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	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	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	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	
Deliberately accessing or trying to access offensive or pornographic material		X	X			X	X		X

Incident	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X	X		X

Staff   Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
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		
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		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X				X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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 / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system		X				X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X		X			X	X
Breaching copyright or licensing regulations		X				X		

Continued infringements of the above, following previous warnings or sanctions			X				X	X

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):…………………………………………
where appropriate

Signed (parent): …………………………………………..

Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
•   that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
•   that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
•   that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name		Pupil Name	

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Signed		Date	

Evergreen Primary School
Online Safety Policy

Staff and Guest Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that staff, visitors and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE e.t.c.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT **systems:**
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.

Evergreen Primary School
Online Safety Policy

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. Staff should be aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

School and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices e.t.c.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.
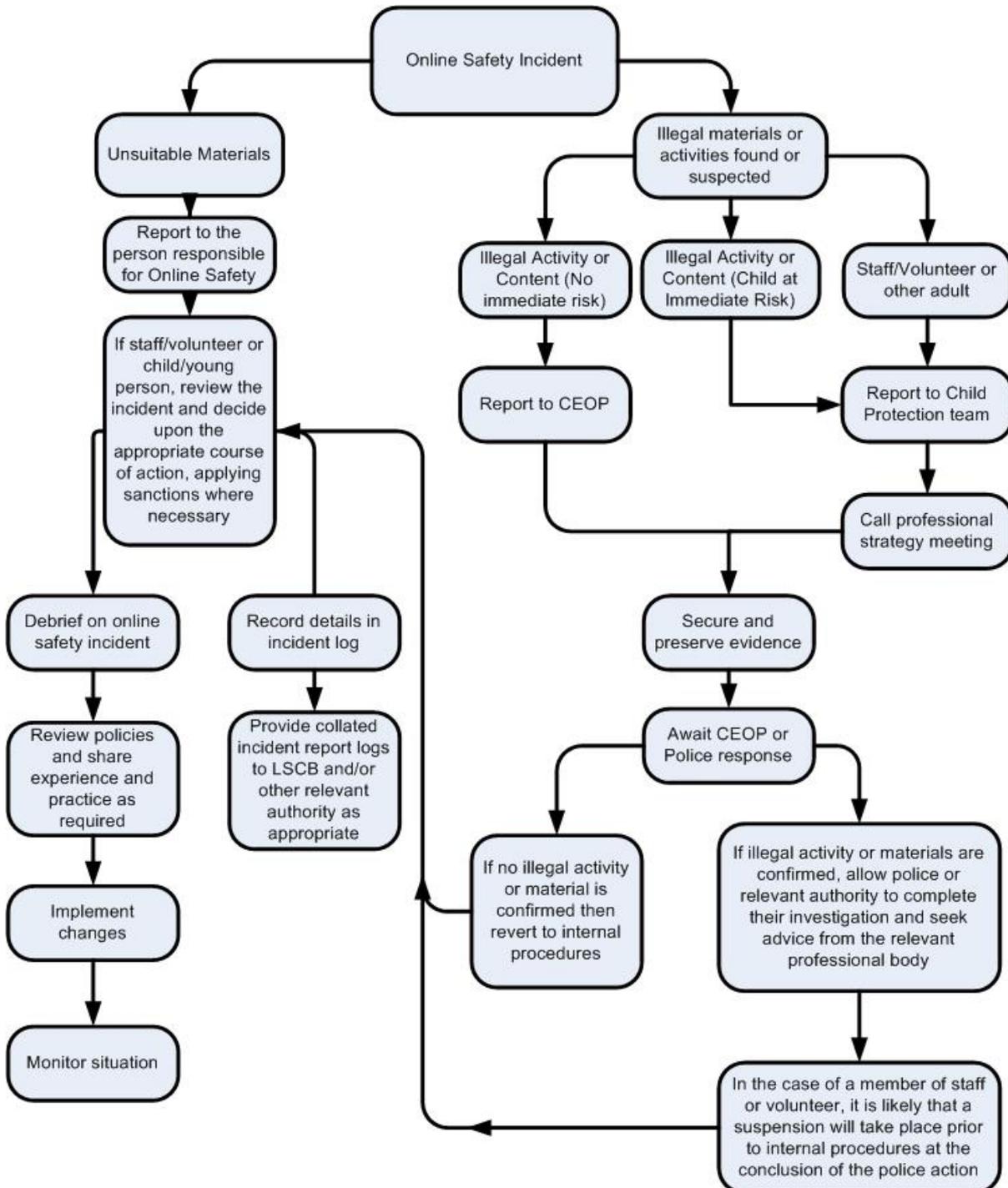

Staff / Volunteer Name   Signed   Date

Responding to incidents of misuse – flow chart

Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to CEOP

Report to Child Protection team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Evergreen Primary School
Online Safety Policy

E-safety incident	Outline :					
Name of member of staff (Discovering the incident)			Date			
Child(ren) involved. (or other adults if no children involved)			Time			
Device(s), Websites, Usernames..						Note:- If there is a possibility of legal action the device should be disconnected and powered down. Do not investigate device as this will damage / remove any evidence. Obtain Police advice.
Nature of incident	Accidental access to inappropriate material	Intentional access to inappropriate material	Creating / Distributing inappropriate Images	Cyber Bullying	Grooming	Other
Details						
The event occurred Location	During a lesson		In unsupervised time	Outside school hours		
Does the even warrant direct Police involvement (Yes if…)	Grooming	Violent image(s)	Pornographic image(s)	Illegal Images	Blackmail	Other criminal activity
Police Involvement	Yes/No	Date & Time	Contact			
LADO Involvement	Yes/No	Date & Time	Contact			

Head of School - Safguarding Contact				
(Staff)	Contact made with SGSS / Personnel	Recommended action	Action applied	Chair of Govs contacted
Other Children	Contacted Parents (names)		Date	Time
	Interviewed Parents/Carers Name / Date / Time	Other Interviews Name / Date / Time		Append notes of interviews)
Potential Technical Changes				Completed
Potential Teaching Changes				Completed

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Gavin Thompson – School Technician.

Technical Security

Policy statements

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 will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users will have clearly defined access rights to school technical systems.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and

must immediately report any suspicion or evidence that there has been a breach of security.

- Gavin Thompson - technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place as described in the esafety policy for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician.
- An agreed policy is in place as described in the esafety policy for the provision of temporary access of trainee teachers, supply teachers onto the school system.
- An agreed policy is in place as described in the esafety policy regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place as described in the esafety policy 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 as described in the esafety policy regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements
- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager Technician and will be reviewed, at least annually, by the Online Safety Committee.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school / academy systems, used by the technical staff must also be available to the Headteacher or Head of School and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by Gavin Thompson (technician. Any changes carried out must be notified to the manager of the password security policy (above).

- All users (adults and pupils) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account
- requests for password changes should be authenticated by Gavin Thompson to ensure that the new password can only be passed to the genuine user.

Staff passwords:
- **All staff users will be provided with a username and password** by Gavin Thompson IT Techinician who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 90 days
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Student / pupil passwords

- All users will be provided with a username and may be given a password where appropriate depending on their cognitive ability by Gavin Thompson – Technician.
- Users with passwords will be required to change their password every term.
- Students / pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:
- at induction / staff meetings/ briefings
- through the school's Online Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:
- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person – Gavin Thompson will ensure that full records are kept of:
- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Filtering

Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by Gavin Thompson. He will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems and communicate them to the Head of School

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to a second responsible person Judith Benson**:**
- either... be reported to and authorised by a second responsible person Judith Benson prior to changes being made
- be reported to the Online Safety Group

All users have a responsibility to report immediately to Deborah Scurr /Sarah Phillips any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider ITSS DCC
- The school has provided enhanced / differentiated user-level filtering through the use of the Lightspeed Systems Web Filter allowing different filtering levels for different groups of users – staff / pupils.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of School
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider Lightspeed Systems.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:
- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter.

Changes to the Filtering System

The school technician Gavin Thompson and Head of School have access to change filtering systems
- Any member of staff can request changes to the filtering system verbally.
- The request will be discussed and considered by the Senior Leadership Team
- The Head of School will be involved to provide checks and balances this person will be a member of the SLT (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)
- Lightspeed has an audit log which registers any changes made to the filter

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to The Head of School who will decide whether to make school level changes (as above).

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting
Logs of filtering change controls and of filtering incidents will be made available to:

- The Head of School
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Legislation
Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:
- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
• Establish the facts;
• Ascertain compliance with regulatory or self-regulatory practices or procedures;
• Demonstrate standards, which are or ought to be achieved by persons using the system;
• Investigate or detect unauthorised use of the communications system;
• Prevent or detect crime or in the interests of national security;
• Ensure the effective operation of the system.
• Monitoring but not recording is also permissible in order to:
• Ascertain whether the communication is business or personal;
• Protect or support help line staff.
• The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

•   Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

•   Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

•   The right to a fair trial

•   The right to respect for private and family life, home and correspondence

•   Freedom of thought, conscience and religion

•   Freedom of expression

•   Freedom of assembly

- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Links to other organisations or documents
The following links may helpful when implementing developing the school Online Safety policy.

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/   ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz   http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support   SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN   - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL -   Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational Online Safety programmes for schools, young people and parents.

VLE   Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP   Wireless Application Protocol

Policy reviewed by Children's Committee

Signed …………………………. Mr R Patel (Chair)

Date 28th June 2017

Due for review: Summer 2018