## E-Safety and Online Policy

| Required Review Frequency | Every 3 years – FGB to determine |
|---|---|
| Next Review Due: | May 2024 |
| Committee Responsible: | Curriculum & Standards Committee |
| Document Location | School |

| Version | Approved By | Date of Approval | Key Changes |
|---|---|---|---|
| 1.0 | FGB | 19/05/2021 | New policy is a merger of the LA model E-safety policy and the previous Online policy |

# 1. Scope of the Policy- Principles of E Safety

1.1 This policy applies to all members of St Helen's Primary School (including staff, pupils, volunteers, parents/carers, visitors, governors and community users) who have access to and are users of IT systems, both in and out of the school.

1.2 The Education and Inspections Act 2006 empowers Headteachers 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 E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.  The Education Act 2011increased these powers with regard to the searching for and viewing of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published School Behaviour Policies.

1.3 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 E-Safety behaviour that take place out of school.

# 2. Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school for E safety.

## 2.1 Governors:

2.1.1 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding *Governor,*  Hannah Straine-Francis, *who will report back to the Curriculum and Standards Committee* receiving regular information about E-Safety incidents and monitoring reports. As a member of the Governing Body

the Safeguarding Governor has taken on the role *of E-Safety Governor.* The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator (at least 3 per year)
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors at Curriculum and Standards committee.

## 2.2 Executive Head, Head of School and Senior Leaders:

2.2.1 The Head of school has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator who is the DSL Kelvin Chappell.

2.2.2 The Head of School and all other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (See flow chart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR).

2.2.3 The Executive Head Teacher and Head of School are responsible for ensuring that other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

2.2.4 The Executive Head Teacher 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 E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

2.2.5 The Senior Leadership Team will receive regular monitoring reports from the DSL, who is the E-Safety Co-ordinator.

## 2.3 E-Safety Coordinator/Officer:

2.3.1 The E-Safety Coordinator is Kelvin Chappell. Their role is to:

- ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- liaise with the Local Authority/other relevant bodies
- liaise with school technical staff
- receive reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments. (These logs are maintained on CPOMS)
- meet 3 times per year with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs (E-safety Governor will fall under the remit of the Safeguarding Governor)
- attend relevant meetings/committees of Governors
- report regularly to Senior Leadership Team

## 2.4 Computing Subject Leader:

2.4.1 The Computing Subject Leader is Liz Pearce. Their role in E-Safety is to:

- take day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the school E-Safety policies /documents alongside the DSL
- provide training and advice for staff
- plan the school's E-Safety scheme of work, including the annual E-Safety week **(E safety scheme of work is taught in Term 1 as part of the South Glos Integra Computing Scheme of Work.)**
- liaise with the Local Authority
- liaise with school technical staff
- meet with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs,
- when necessary, attend relevant meetings/committees of Governors

## 2.5 Technical staff:

2.5.1 The Network Manager/Technical Staff is provided through Integra IT services, and they 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 E-Safety technical requirements and any Local Authority/other relevant body E-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 LA 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 E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

## 2.6 Teaching and Support Staff

2.6.1 Teachers and support staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Executive Head Teacher and Head of School /Chair of Governors/LADO for investigation/action/sanction
- all digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-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 (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

## 2.7 Designated Safeguarding Officer

2.7.1 The Designated Safeguarding Officer is Kelvin Chappell. The Deputy Designated Safeguarding Officer is Andrew Spens.  The Designated Safeguarding Officer should be trained in E-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

## 2.8 Pupils:

2.8.1 All Pupils at St Helen's Primary School:

- are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Policy
- should 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 (covered as part of Term 1 Computing)
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

2.8.2 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 E-Safety campaigns/literature.  Parents and carers will be encouraged to support the school in promoting good E-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 on-line student/pupil records
- their children's personal devices in the school

## 3. Policy Statements

## 3.1 Education – pupils

3.1.1 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 E-Safety is therefore an

essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

3.1.2 E-Safety and learning about online safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and informed by the following:

- a planned E-Safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- key E-Safety messages should be reinforced as part of a planned programme of assemblies
- 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

## 3.2 Education – parents/carers

3.2.1 Many parents and carers have only a limited understanding of E-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.

3.2.2 The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents' Workshops
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

## 3.3 Education – The Wider Community

3.3.1 The school will provide opportunities for local community groups/members of the community to gain from the schools/academy's E-Safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide E-Safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their E-Safety provision

## 3.4 Education & Training – Staff/Volunteers

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

• A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out annually
• All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements
• The Computing Subject Leader 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 E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
• The Computing Subject Leader will provide advice/guidance/training to individuals as required
  • All volunteers in school are briefed on the school's safeguarding protocols and this includes be vigilant around and E-safety issues that may arise.

## 3.5 Training – Governors

3.5.1 Governors/Directors should take part in E-Safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/E-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 (e.g. SWGfL)
• Participation in school training/information sessions for staff or parents

## 4. Technical – infrastructure/equipment, filtering and monitoring

4.1 The school alongside Integra IT 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 E-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 academy 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
• All users will be provided with a username and secure password by the network engineers 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/IT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)

- Integra IT 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 (including child sexual abuse images) is filtered by the broadband or filtering provider by 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
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc.)
- 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 for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- 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 (guest logins) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school (See AUP)
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices (See AUP)
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (See AUP)

Internet Provider and Filtering
Internet access is filtered for all users by Integra IT and our school is currently implementing a technical monitoring solution (iBoss) through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. The iBoss solution provides the following:

- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Integra IT to support the school by drawing attention to concerning behaviours, communications or access
- enhanced filtering integrated with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office
- delegated access to the filtering system allows us to permit or deny access to specific content to support the requirement that "over blocking" does not lead to unnecessary restrictions on what can be taught relating to online teaching and safeguarding - the most severe content will always be filtered
- network level filtering which does not rely on any software on the users' devices which could be disabled
- ability to produce reports on the websites visited by all young people and adults using our systems
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up
- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail
- ability to log in from anywhere to see reports via web interface

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

Technical staff monitor internet traffic and report any issues to schools.

The school reports issues through logging a call to the service desk at 01454 863838.

# 5. Use of digital and video images

5.1 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
- 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 in 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
- 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 (See Staff Acceptable Use Policy). When staff have used their personal device to record video/ images, they will delete the image as soon as they have saved it to, for example, Twitter, etc. 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 anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or elsewhere
- Pupil's work can only be published with the permission of the pupil and parents/carers

# 6. Data Protection

6.1 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

6.2 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" (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act
- 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

6.3 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

6.4 When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

# 7. Communications

7.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

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

7.2 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 others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person – 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 (email etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications with parents/ carers. Communication channels must involve Emails or through Class Dojo applications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above may be provided with individual school email addresses for educational use if the need arises.
- Pupils should be taught about E-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

## 8. Social Media - Protecting Professional Identity

8.1 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, 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

8.2 School staff, Governors and Volunteers 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.

8.3 The school's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

## 9. Unsuitable/inappropriate activities

9.1 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:

## User Actions

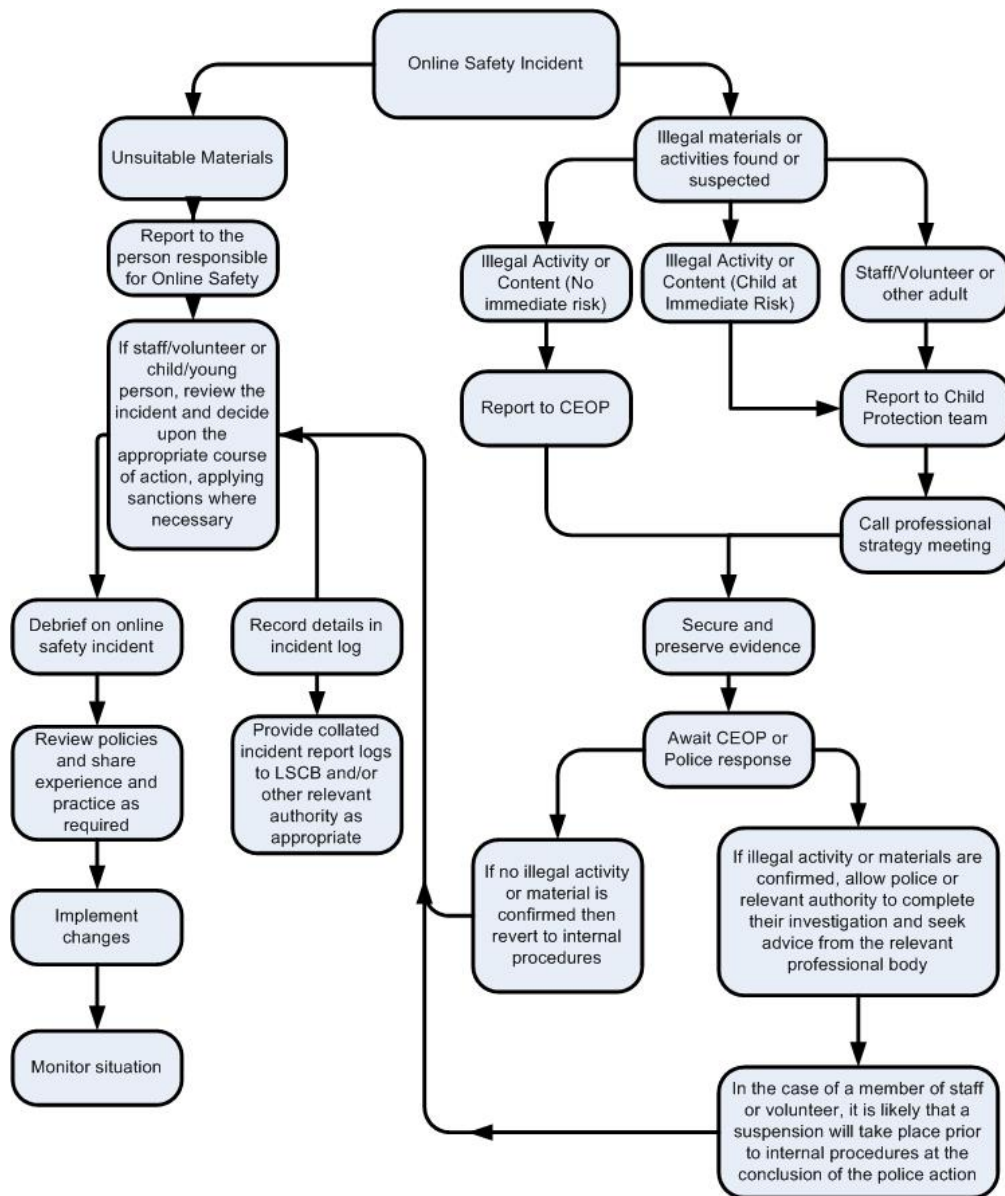| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, | Child sexual abuse images –The making, production or distribution of indecent images 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 |

| | | | | | | |
|---|---|---|---|---|---|---|
| download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | 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 (e.g. 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 | | | **X** | | | |
| File sharing | | | | **X** | | |
| Use of social media | | | X | | | |
| Use of messaging apps | | | X | | | |
| Use of video broadcasting e.g. Youtube | | | X | | | |

# 10. 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).

## 10.1 Illegal Incidents

10.1.1 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.

**Online Safety Incident**

Branch 1: **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

Branch 2: **Illegal materials or activities found or suspected**
- Illegal Activity or Content (No immediate risk) → Report to CEOP
- Illegal Activity or Content (Child at Immediate Risk) → Report to Child Protection team
- Staff/Volunteer or other adult → 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

## 10.2 Other Incidents

10.2.1 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.

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

- Have more than one senior member of staff/volunteer 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

10.2.3 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.

10.2.4 Sexting - is becoming more common. Sexting is described as the "generation of video and/or images that are indecent or of a sexual nature by children under the age of 18."
Pupils will be encouraged to report all incidents of sexting. Teaching staff will inform the Designated Officer for Safeguarding who will act according to the Safeguarding Policy and the guidance outlined in the "Sexting" in schools: advice and support around self-generated images 2013 document.

## 10.3 School Actions & Sanctions

10.3.1 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:

## Pupils                                         Actions/Sanctions

| Incidents: | Refer to class teacher | Refer to Phase Leader/ SLT | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Warning | Further sanction e.g. 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 | |
| Unauthorised use of mobile phone/digital camera/other mobile device | | | X | | | X | | | |
| Unauthorised use of social media/ messaging apps/personal email | | | X | | | X | | | |
| Unauthorised downloading or uploading of files | | | X | | | X | | | |
| Allowing others to access school network by sharing username and passwords | | | X | | | X | X | | |
| Attempting to access or accessing the school network, using another student's /pupil's account | | X | | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | | | X | | | X | X | | X |
| Corrupting or destroying the data of other users | | | X | | | X | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | | 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 |
| Using proxy sites or other means to subvert the school'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 |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | | X | | | X | | | X |

## Staff                                   Actions/Sanctions

| Incidents: | Refer to line manager | Refer to Head of School | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | 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 | | | 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 e.g. holding or transferring data in an insecure manner | | X | | | X | | | |
| Deliberate actions to breach data protection or network security rules | | X | | | | X | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | 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 | X |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils | | | X | | | X | X | |
| Actions which could compromise the staff member's professional standing | | X | 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 | | |
| 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 | | X | X | | | | | X |

**Self-evaluation and Improvement**
The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:
•       Local authority safeguarding audit
•       360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.

- Surveys with pupils and staff when necessary to do so.

# Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

# 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 E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

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

Copyright of these Template Policies is held by SWGfL. Schools/Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development.  Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.