Online Safety Policy

Contents

2

Development / Monitoring / Review of this Policy

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

- **Headteacher & Senior Leaders**
- **Online Safety Officer**
- **Staff – including Teachers, Support Staff, Technical staff**
- **Governors / Board**
- **Parents and Carers**
- **Community users**

Consultation with the whole academy 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 Board of Directors / Governing Body Committee on:	**Awaiting Review**
The implementation of this Online Safety policy will be monitored by the:	**Computing Lead** **E-safety lead** **Senior Leadership Team** **Safeguarding Governor**
Monitoring will take place at regular intervals:	**June (yearly)**
The Board of Directors 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:	**June (yearly)**
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:	**June (yearly)**
Should serious online safety incidents take place, the following external persons / agencies should be informed:	**ICO** **Police** **CEOP**

The school will monitor the impact of the policy using: (delete / add as relevant)

- **Logs of reported incidents**
- **Monitoring logs of internet activity (including sites visited) / filtering**

- **Internal monitoring data for network activity**
- **Surveys / questionnaires of**
    - **students**
    - **parents / carers**
    - **staff**

Scope of the Policy

This policy applies to all members of the school community (including staff, students, 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 Headteachers to such extent as is reasonable, to regulate the behaviour of students 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. 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 behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

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 E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor and e-safety will be overseen as part of this role.

The role of the Online Safety Governor

- **regular meetings with the Online Safety Co-ordinator / Officer**
- **attendance at Online Safety Group meetings**
- **regular monitoring of online safety incident logs**
- **regular monitoring of filtering / change control logs**
- **reporting to relevant Governors / Board / Committee / meeting**

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator / Officer.**
- **The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse"**
- **The Headteacher and Senior Leaders 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.**
- **The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. 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 / Officer:

- **leads the Online Safety Group**
- **takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents**
- **ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.**
- **provides training and advice for staff**
- **liaises with the Local Authority / relevant body**
- **liaises with school technical staff**
- **receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,**

- **meets regularly with Online Safety Governor / Director to discuss current issues, review incident logs and filtering / change control logs**
- **attends relevant meeting / committee of Governors**
- **reports regularly to Senior Leadership Team**

Network Manager / Technical staff:

The Network Manager Computing is responsible for ensuring:

- **that the schools technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required online safety technical requirements**
- **that users may only access the networks and devices through a properly**
- **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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Senior Leader; Online Safety Coordinator for investigation**
- **that monitoring software (Impero) are implemented and updated as agreed in school policies**

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 / Agreement (AUP)**
- **they report any suspected misuse or problem to the Headteacher; Online Safety Coordinator for investigation**
- **all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems**
- **online safety issues are embedded in all aspects of the curriculum and other activities**

- **students understand and follow the Online Safety Policy and acceptable use policies**
- **students 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 students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches**

Designated Safeguarding Lead / Designated Person / Officer

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

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

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. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator / Officer (or other relevant person, as above) with:

- **the production / review / monitoring of the school Online Safety Policy / documents.**
- **the production / review / monitoring of the school filtering policy (if the school chooses to have one) 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 students about the online safety provision**

Students:

- **are responsible for using the school digital technology systems in accordance with the age appropriate Student Acceptable Use Agreement**
- **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 / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- **digital and video images taken at school events**
- **access to parents 'sections of the website and on-line student Community Users**

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 should be provided as part of Computing should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.**
- **Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**

- **Students should be helped to understand the need for the student / 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.**
- **It is accepted that from time to time, for good educational reasons, students may need to research topics (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, Learning Platform**
- **Parents / Carers evenings / sessions**
- **High profile events / campaigns e.g. Safer Internet Day**
- **Reference to the relevant web sites / publications e.g. swgfl.org.uk**

Education – The Wider Community

The school will 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 e.g. Early Years Settings, Childminders, youth / sports / voluntary 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 regularly.**

- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- **It is expected that some staff will identify online safety as a training need within the performance management process.**
- **The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL 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 / team meetings / INSET days.**

Training – Governors

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

- **Attendance at training provided by the relevant organisation (e.g. SWGfL).**
- **Participation in school training / information sessions for staff and 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(June yearly)**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**

- **All users will be provided with a username and secure password by who will keep an up to date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password termly.**
- **The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (eg school safe)**
- **Network manager 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 or filtering provider. 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**
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- **The school has provided enhanced and differentiated user-level filtering allowing different filtering levels for different groups of users – staff / students.**
- **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 (Impero) 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 (Staff and volunteers) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.**
- **An agreed policy is in placec that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.**

- **An agreed policy is in place (regarding the use of removable media (eg 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.**

Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behavior Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education progra.

- **The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No	No	No
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	No	No
No network access				No	No	No

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press**
- **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 students in the digital / video images.**
- **Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.**
- **Students must not take, use, share, publish or distribute images of others without their permission**
- **Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.**
- **Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.**

- **Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.**

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR law which states that personal data must be:

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 (see appendix for template policy)**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- **Responsible persons are appointed / identified - Senior Information Risk Officer (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 transfer / 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 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**

Communications

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:

Communication Technologies	Staff & other adults				Students			
	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 the 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	X				X			
Use of personal email addresses in school , or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps	X							X
Use of social media	X							X
Use of blogs	X				X			

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 students 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 students or parents / carers (email, social media, blogs, Microsoft Teams 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.

- Whole class / group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.
- Students 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 group 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:

- Training is provided including: 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 students , 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- **Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.**
- **Systems for reporting and dealing with abuse and misuse**
- **Understanding of how incidents may be dealt with under school disciplinary procedures**

Monitoring of Public Social Media

- **As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school**
- **The school should effectively respond to social media comments made by others according to a defined policy or process**

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

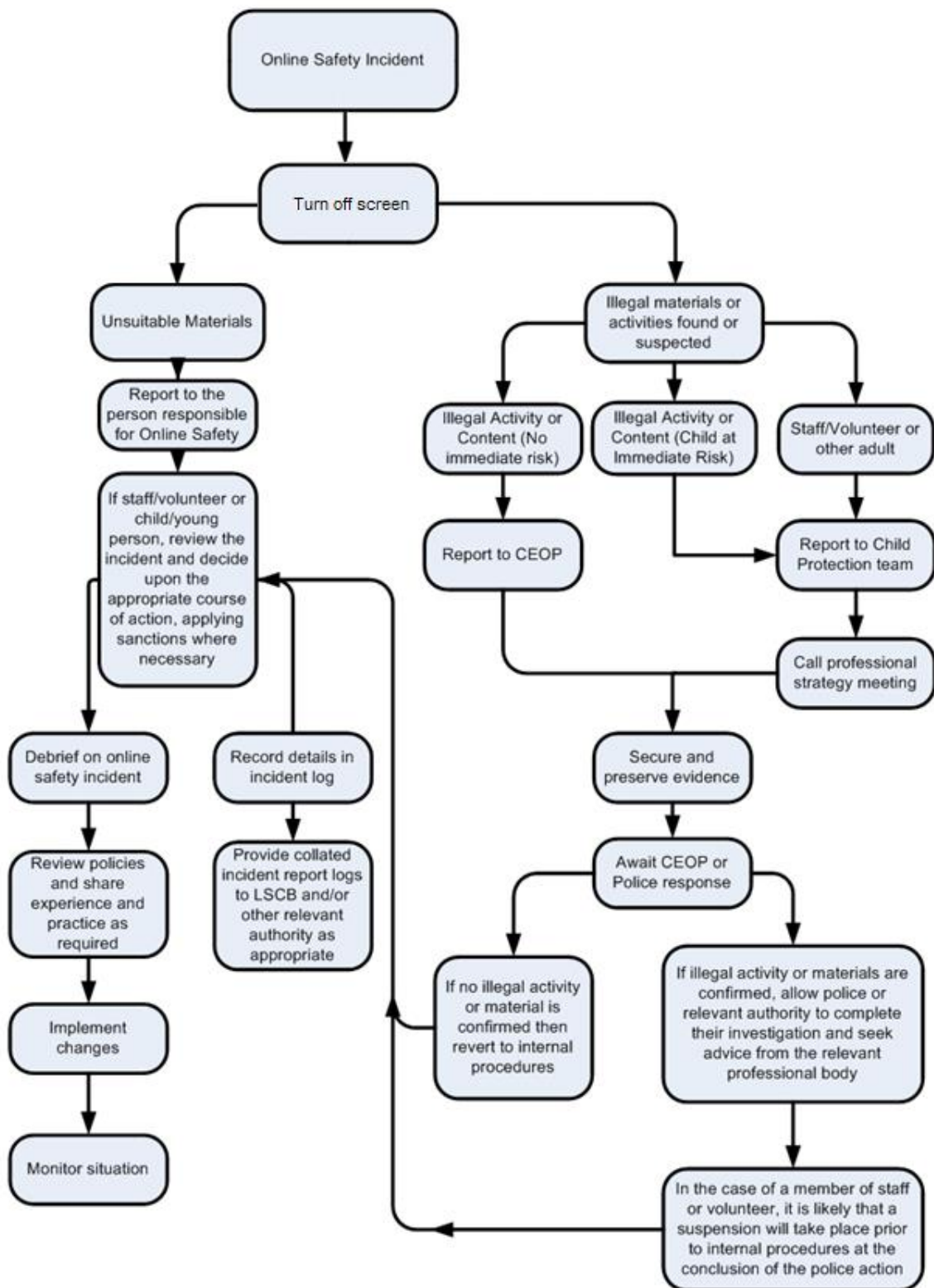| User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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	
Promotion of extremism or terrorism				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				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			x		
File sharing		x			
Use of social media			x		
Use of messaging apps		x			
Use of video broadcasting e.g. 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 for responding to online safety incidents and report immediately to the police.

```
                          ┌─────────────────────┐
                          │ Online Safety Incident │
                          └──────────┬──────────┘
                                     │
                          ┌──────────┴──────────┐
                          │     Turn off screen  │
                          └──────────┬──────────┘
```

Online Safety Incident

Turn off screen

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

Record details in incident log

Review policies and share experience and practice as required

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

Implement changes

Monitor situation

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

23

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 / 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 Group or national / local organisation (as relevant).**
  - **Police involvement and/or action**
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - **incidents of 'grooming' behaviour**
  - **the sending of obscene materials to a child**
  - **adult material which potentially breaches the Obscene Publications Act**
  - **criminally racist material**
  - **promotion of terrorism or extremism**
  - **other criminal conduct, activity or materials**
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students Incidents	Refer to class teacher / tutor	Refer to Head phase	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
				Actions / Sanctions					
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		x	x		
Unauthorised use of non-educational sites during lessons	x	x				x		x	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x				x		x	
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x			x	x		x	
Unauthorised downloading or uploading of files	x	x			x	x		x	

Allowing others to access school network by sharing username and passwords	x						x	
Attempting to access or accessing the school network, using another student's / pupil's account	x	x			x			
Attempting to access or accessing the school network, using the account of a member of staff	x		x		x	x	x	x
Corrupting or destroying the data of other users					x			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x			x	x	x	
Continued infringements of the above, following previous warnings or sanctions	x	x	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		x	x
Using proxy sites or other means to subvert the school's 's filtering system	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		x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					x			

	Actions / Sanctions							
Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to 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		X	X	X		x		
Inappropriate personal use of the internet / social media / personal email		x						
Unauthorised downloading or uploading of files								

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x					x		
Deliberate actions to breach data protection or network security rules		x	x			x		x
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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		x	x			x		x
Actions which could compromise the staff member's professional standing	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 's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident					x			
Deliberately accessing or trying to access offensive or pornographic material		x	x		x	x		x
Breaching copyright or licensing regulations			x			x		
Continued infringements of the above, following previous warnings or sanctions		x	x					x

Appendix

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

http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-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 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**

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 writing, 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.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2016