Online Safety Policy

Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
Our school online policy helps to ensure safe and appropriate use of ICT by children at all times.

Development and Monitoring

This online safety policy has been developed by members including the Head teacher, ICT subject leader, deputy safeguarding officer, non-teaching staff member, governor and parent.

Consultation with the whole school community has taken place through the following:

- Staff meetings
- INSET day
- Governor meeting/sub committee meeting
- Parents evenings

The school will monitor the impact of the policy using:

• Logs of reported incidents
• SWGfL monitoring logs of internet activity (including sites visited)
• Internal monitoring data for network activity
• Surveys / questionnaires of - pupils (eg CEOP ThinkUknow survey)
parents/carers
staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
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 online-bullying, or other online safety incidents covered by this policy.
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 onlinonline safety behaviour that take place out of school.

Schedule for Development / Monitoring / Review

The policy will be monitored and reviewed annually. The Computing Subject Leader will report back to the DSL who will take the appropriate action required. Any incidents will be reported to full governors as part of the termly safeguarding data collection report.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Full Governing Body receiving regular information about online safety incidents and monitoring reports will carry this out. 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 Computing Subject Leader
- regular monitoring of online safety incident logs
- reporting to relevant Governors meeting

Head teacher, ICT Coordinator and Nominated Governor:

• The Head teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be shared with the ICT coordinator.

• The Headteacher and member of the Governing Body 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 SWGfL flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR /disciplinary procedures)

• that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Onlinonline safety Policy and guidance

• that users may only access the school's networks through a properly enforced password protection policy

The company Alchemy and SWGfL are responsible for ensuring:

• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

Online safety/Computing Subject Leader

•leads the online safety committee

•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 and technical support (Alchemy)

•receives 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 meeting / committee of Governors
•ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
•ensures that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
•ensures that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
•SWGfL is informed of issues relating to the filtering applied by the Grid

Teaching and Support Staff:

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 school Acceptable Internet Use Statement.
• they report any suspected misuse or problem to the Head teacher, ICT Co-ordinator or Nominated Governor
• digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
• pupils understand and follow the school online safety and acceptable use policy
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor the use of digital technologies, mobile devices, cameras, etc in lessons and other school activities (where allowed), and implement current policies with regard to these devices.
• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead / Child Protection Officer

•should be trained in online safety issues and be aware of the potential for serious child protection 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
•online-bullying

Pupils:

Pupils are responsible for ensuring that:

• they use the school digital technology systems in accordance with the Pupil Acceptable Use Statement, which they will be expected to sign before being given access to school systems.

•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 school policies on the use of mobile devices, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online -bullying.

•should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about online safety campaigns. Parents/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 / VLP and on-line student / pupil records

Community Users:

Community Users who access school ICT systems/ website as part of the Extended School provision will be expected to sign an Community Use Agreement 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 digital literacy 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 programme should be provided as part of Computing/PSHE/literacy lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
• Key online safety messages could be reinforced as part of assemblies.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
• Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
• Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
• Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:
• Letters, newsletters and website
• Curriculum activities
• Parents evenings/sessions/assemblies
• High profile events/campaigns e.g. Safer Internet Day
• Reference to the relevant websites/publications, e.g. www.swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

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:

- 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

Education & Training – Staff and Governors

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:
• The school will ensure that all staff are up to date with online safety procedures. Training will be made available as and when appropriate. (minimum of an annual update)
• All new staff will receive the Acceptable Use Policy as part of their induction programme.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance.

• All users will have clearly defined access rights to school technical systems and devices.

•Servers, wireless systems and cabling must be securely located and physical access restricted.

• All users (at KS2) will be provided with a username and secure password by the ICT coordinator 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 annually.

• The "administrator" passwords for the school ICT system, must also be available to the Headteacher and kept in a secure place.

• The ICT coordinator 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 via SWGfL.

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 / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

	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*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*

Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. There may be events where the school will film or photograph the event and we ask the parents not to film it personally.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should 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 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.
- 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 current data protection legislation.

The school must ensure that:

• It has a Data Protection Policy.
• It has paid the appropriate fee to the Information Commissioner's Office (ICO).
• It has appointed a Data Protection Officer (DPO).
• 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.
• Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
• The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
• Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
• Data Protection Impact Assessments (DPIA) are carried out.
• It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
• Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
• There are clear and understood data retention policies and routines for deletion and disposal of data.
• There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
• Consideration has been given to the protection of personal data when accessed using any remote access solutions.
• All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
• All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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 / academy 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:

	Staff & other adults				Students / Pupils			
Communication Technologies	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 or other camera devices		✓						✓
Use of hand held devices eg PDAs, PSPs		✓						✓
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓	✓			
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

***Used in reference with the adult acceptable use policy and other school policies**

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 need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.

Social Media – Protecting Professional Identity

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, online bully, 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 minimize risk of loss of personal information.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / 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 / academy context and that users, as defined below, should not engage in these activities in /or outside the school when using school equipment or systems. The school policy restricts usage as follows:

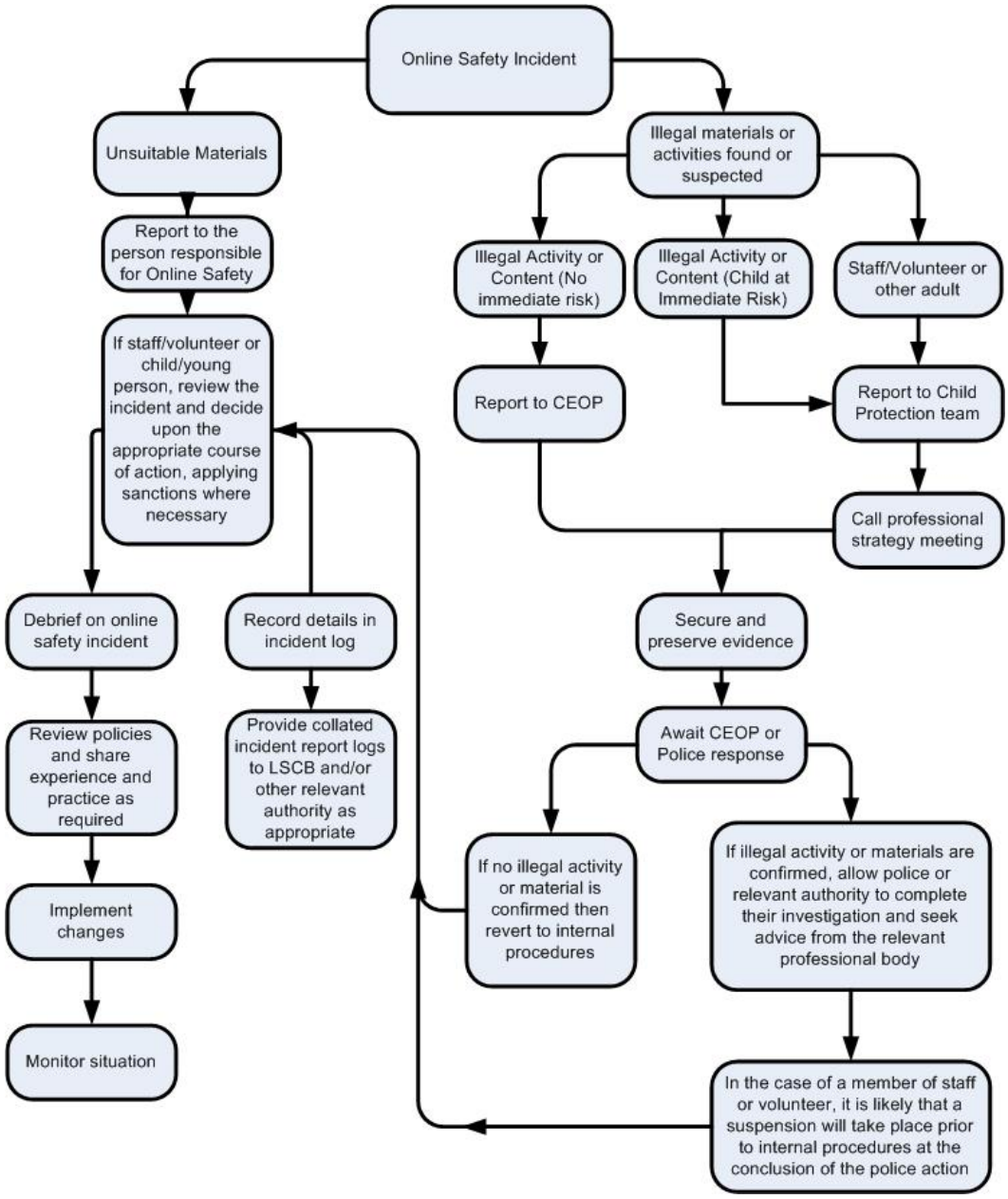
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child 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				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) for responding to online safety incidents and report immediately to the police.



Other incidents

It is hoped that all members of the school community will be responsible users of digital technology, who understand and follow this 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 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

Pupils	Actions/Sanctions								
Incidents	Refer to class teacher	Refer to Head of Department	Refer to Head teacher	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 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		X		X	
Unauthorised use of non-educational sites during lessons	X	X	X		X	X		X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X		X	X		X	
Unauthorised use of social media / messaging apps / personal email	X	X	X		X	X		X	
Unauthorised downloading or uploading of files	X	X	X			X		X	
Allowing others to access school / academy network by sharing username and passwords	X	X	X			X		X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X			X		X	
Attempting to access or accessing the school / academy 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	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions	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	
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X			

School Actions & Sanctions (cont.)

Staff Actions/Sanctions

Incidents	Refer to line manager	Refer to Head teacher	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	X		X		X
Inappropriate personal use of the internet / social media / personal email		X				X		X
Unauthorised downloading or uploading of files		X				X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		X
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		X
Deliberate actions to breach data protection or network security rules	X	X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		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	X			X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X	X			X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X			X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions	X	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