



# Online Safety Policy

March 2017

# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee

- Headteacher
- Senior Leadership Team
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users

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

## Schedule for Development / Monitoring / Review

This Online Safety policy was approved by Governing Body on	
The implementation of this Online Safety policy will be monitored by the:	<i>– Online Safety Coordinator Headteacher Computing Coordinator</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Annually</i>
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:	<i>Annually or when significant changes are required</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Online Safety Coordinator Designated Safeguarding Lead Safeguarding Officer, LADO, Police</i>

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers 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 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 Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor / Director will include:

- regular meetings with the Online Safety Co-ordinator, 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.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).
- 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 / Senior Management Team will receive regular monitoring reports from the Online Safety Co-ordinator.

## Online Safety Coordinator

- 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 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 ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / 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 / action / sanction
- that monitoring software / systems 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 / academy Online Safety Policy and practices
- they have read, understood Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems

- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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 Leads

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 / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

## Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (as age appropriate, e.g. Upper Key Stage Two).

- 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 (as age appropriate, e.g. Upper Key Stage Two).
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

## Community Users

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

## Policy Statements

### Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's / academy'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 / PHSE other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation (Please see Preventing Radicalisation Policy for further information)
- 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.

## 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, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Signpost to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  
<http://www.childnet.com/parents-and-carers> (see appendix for further links / resources) These will be found on school website

## 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

## 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:

- 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 (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## 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:

- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

## 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 / academy meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- All users (at KS2 and above) will be provided with a username and secure password by (Computing 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.
- The “master / administrator” passwords for the school / academy 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)
- The 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licencing costs)
- **Internet access is filtered for all users.** Illegal content (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 (see appendix for more details)
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.** *Nb. additional duties for schools / academies under the Counter Terrorism and*

*Securities Act 2015 which requires schools / academies to ensure that children are safe from terrorist and extremist material on the internet*

- 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 (BYO Device Policy) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- *An agreed policy is in place 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 / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour 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 programme.

- **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 <sup>1</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes Year 4 upwards	Yes	Yes/
Full network access	Yes	Yes	No	No	No	No
Internet only			Yes	No	Yes	Yes
No network access						

---

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

# Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press / Tapestry for the EYFS – signed for letter given as part of admissions.
- 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 students / 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. 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 student / pupil and parents or carers.

## 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:

<i>Communication Technologies</i>	<i>Staff and other adults</i>				<i>Pupils</i>			
	<i>Allowed</i>	<i>Allowed at certain times</i>	<i>Allowed for selected staff</i>	<i>Not allowed</i>	<i>Allowed</i>	<i>Allowed at certain times</i>	<i>Allowed with staff permission</i>	<i>Not allowed</i>
<i>Mobile phones may be brought to the school</i>	•						•	
<i>Use of mobile phones in lessons</i>			•					•
<i>Use of mobile phones in social time</i>	•							•
<i>Taking photos on mobile phones / cameras</i>				•				•
<i>Use of other mobile devices e.g. tablets, gaming devices</i>	•					•		
<i>Use of personal email addresses in school or on school network</i>	•							•
<i>Use of school email for personal emails</i>		•						•
<i>Use of messaging apps</i>		•						•
<i>Use of social media</i>		•						•
<i>Use of blogs</i>		•					•	

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.
- Users must immediately report, to the nominated person – in accordance with the school
- 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, social media, chat, blogs 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 pupils at KS2 and above will be provided with individual school email addresses for educational use. Parents/Carers will be informed about the use of Google apps by letter. This includes a permission slip which must be returned. (Year 3 to Year 6)
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

# Social Media - Protecting Professional Identity

All schools 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:

- Ensuring that personal information is not published
- 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 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

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

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

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

*The school's use of social media for professional purposes will be checked regularly by Online Safety Group to ensure compliance with the school policies.*

## Unsuitable / inappropriate activities

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

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

		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	
	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					X	

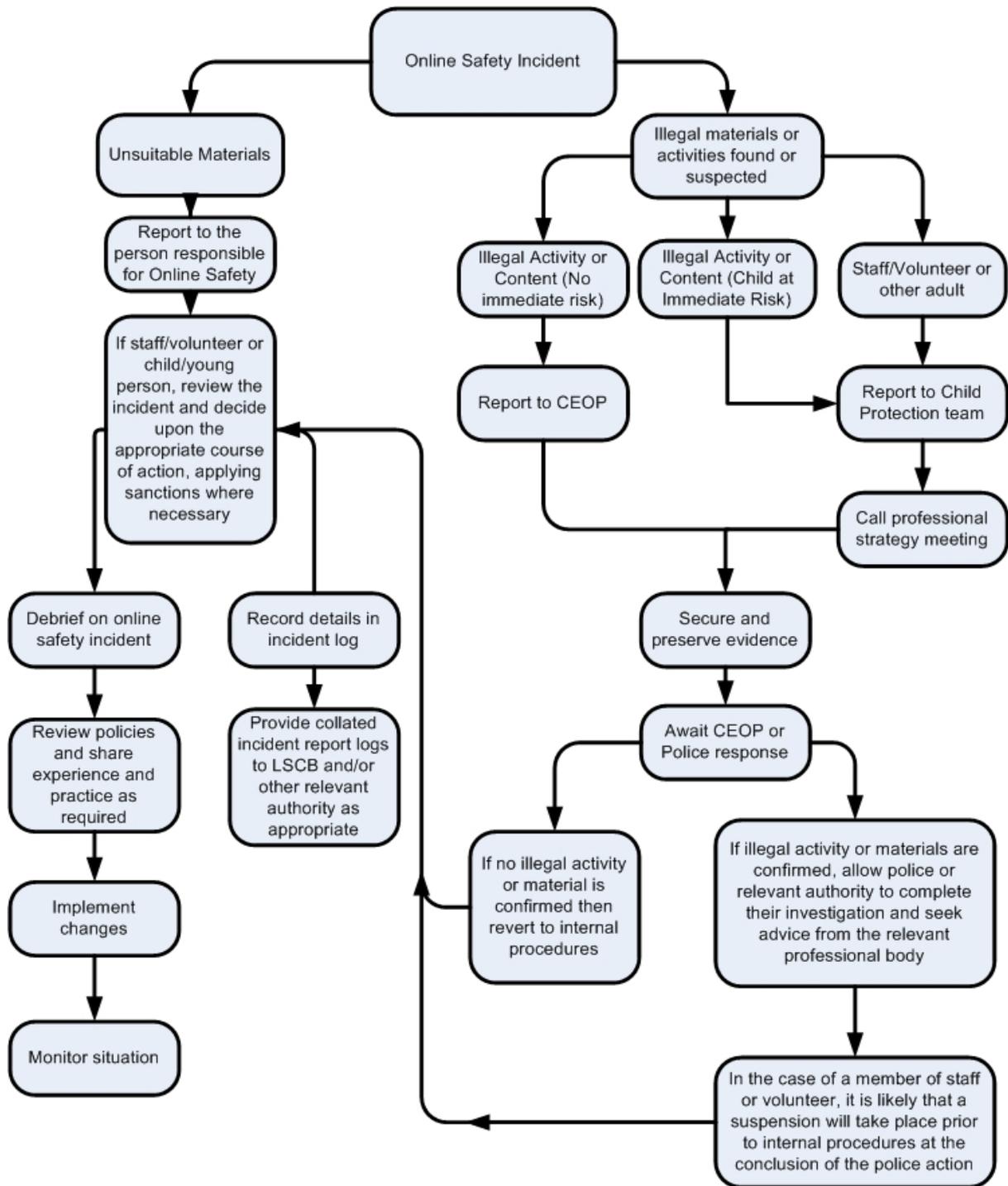
safeguards employed by the school / academy					
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X	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 (below and appendix) for responding to online safety incidents and report immediately to the police.



## Other Incidents

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

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

- Have more than one senior member of staff / 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
  - 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:

### Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher	Refer to Head of Department / Year / other	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons			X			X	X		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device			X			X			X
Unauthorised / inappropriate use of social media / messaging apps / personal email			X			X			X
Unauthorised downloading or uploading of files			X		X	X	X		X
Allowing others to access school / 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	
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	
Actions which could bring the school / academy 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 /			X		X	X	X	X	

academy's filtering system								
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	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X	X	X	X	

### Actions / Sanctions

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

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X					X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X					X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X					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		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

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](mailto: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.

# Appendices

# Pupil Acceptable Use Policy Agreement-KS2

Dear Parents/Carers

## ICT Usage Policy and Agreement

This document has been written to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers including cameras and other devices. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. If you have any questions, please ask your teacher.

Internet use includes accessing the World Wide Web and the use of electronic mail. The school encourages use by pupils of the Internet, together with the development of appropriate skills to analyse and evaluate resources found on it. These skills will be fundamental in the society our pupils will be entering.

## Google Apps for Education

As part of our Computing Curriculum, the school is introducing a service called Google Apps for Education. This new service is powered by Google and we will be joining over 8 million other pupils and teachers that are already using Google Apps at schools around the world. The service will give our children and staff access to a set of tools which will support the high levels of collaboration that are required in today's classroom to prepare students with communication and collaboration skills for life. Apps for Education will also enhance the delivery of not only our Computing curriculum, but lessons cross curricular.

## What's included in Google Apps?

- **Gmail** provides email storage with extra security including *restricted incoming and outgoing email* access. Emails by pupils are restricted to within Withycombe Raleigh's email directory ONLY. These email communications are monitored and recorded. Pupils will NOT be able to send and receive emails outside of our school community unless restrictions are lifted by an administrator for specific teaching purposes.
- **Google Calendar** enables us to create and share school or class calendars with events.
- **Google Docs** lets pupils create and share documents, spreadsheets, presentations, drawings and forms. This also allows pupils to work collaboratively on projects simultaneously in real time. Pupils will be able to work on the same document from their own homes.
- **Google Sites** makes it easy to collect, share, and publish all types of content in a single website. Pupils may also be using sites to create portfolios of work.

## What are the benefits of Google Apps and what's included?

- **Ease of access:** Pupils can access Google Apps at anytime, anywhere. It is designed to work in any browser (Google Chrome, IE, Firefox etc.) and on any computer or tablet. This enables access to your email, calendars and documents (Word, Excel, PowerPoint and Publisher alternatives) from school or at home.
- **Online storage** means that no flash drives (memory sticks etc.) are required with documents and files stored in Google Docs.
- **Collaboration** between students from other classes, schools\*, even different countries\*, working together on group projects. (\*carefully selected and teacher lead). During collaborative work teachers can monitor progress of each child and provide instant written feedback visible to the group or to the individual. This enhances teaching and learning and provides instant and accurate assessment.
- **Online portfolios** of work can be developed by students.

## Within the Withycombe Raleigh Google Apps service:

- There will be no advertisements.
- No external email addresses can contact pupil accounts and vice-versa (unless agreed by the Computing Coordinator eg: pen pals with other schools or password reset emails from carefully selected educational websites).

- All email communication and comments within collaborative work are monitored. This information will be used in conjunction with the behaviour policy.
- Work uploaded to Google Drive remains the property of the creator; it is not copied or kept by Google if it is removed by the creator.

### **User Access**

Pupils will be shown how to use Google Apps within the Computing Curriculum. Pupils will be provided with unique usernames and passwords. Parents/Carers are encouraged to explore Google Apps with their children by logging in together and accessing their school work stored in Google Apps. Pupils will follow school policies for appropriate use when using Google Apps. The service is an extension of the school's own network. Pupils know that the school has the right and ability to monitor user accounts for policy and e-safety purposes as well as having the ability to remove access to some or all Google Apps.

### **Summary for Parents**

Google Apps for Education is an essential part of the curriculum, for all subjects, and pupils without parental permission will be unable to participate in any lessons across the curriculum using Google Apps. All email communication is archived and the school's Acceptable Use Policy will be enforced. School staff will monitor the use of Google Apps when pupils are at school. Parents/Carers are responsible for monitoring their child's use of applications when accessing Google Apps from home. Pupils are responsible for their own behaviour at all times. We are excited to be bringing these tools to the school. Don't hesitate in asking for more information about this decision and how it will impact teaching, learning and communication. This letter can also be found on the school website under "For Parents> Newsletters/Letters".

### **Following these simple rules will help school to keep you safe:**

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- I know that the Internet is provided for pupils to find information, practice skills and communicate with others. It is not for online gaming at school.
- Internet access is a privilege, not a right and that access requires responsibility.
- Unauthorised use of the Internet or use of unauthorised websites will not be tolerated.
- Individual users of the Internet are responsible for their behaviour and communications over the network.
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people.
- Pupils should not expect that files stored on school servers will always be private.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- In addition to the filtering provided by The South West Grid for Learning the school has its own system for filtering individual websites. Any member of the school community can bring a website which causes them concern to the attention of the ICT Coordinator who can arrange for that site to be blocked in school.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not logon using another person's account (with or without their permission.)
- I will think before deleting files.
- I will ask a teacher before printing any document.
- I know that the teachers can, and will, check the files and websites I have used and visited.
- I know that, when using Google Apps, teachers can and will check the emails that I send and receive.
- I will take care when using the computers and other school equipment.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers but NOT other pupils.
- I will not install any software or hardware (including memory sticks) without permission from a teacher.
- I understand that if I am acting inappropriately or don't follow the rules my access to some or all ICT resources can be suspended. A child who is unable to follow the above rules will be dealt with in accordance with the school's Behaviour Policy.

*Keep this at home, perhaps near your home computer ↑*

---

Return this section to school ↓

**ICT Usage Policy and Agreement**

**Pupil:** I agree to the ICT Usage Policy and Agreement Rules and understand the consequences for not following them.

**Parent:** I give my consent for my child to use Google Apps and the secure internet in school. I fully support the school and will promote good e-citizenship at home.

I understand that my child is responsible for their own ICT use in school. I know that my child has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

<b>Pupil Name:</b>	<b>Date:</b>
--------------------	--------------

**Pupil Signature:**

**Parent/Guardian Signature:**

**Parent/Guardian Name (Printed)**



# Pupil Acceptable Use Policy Agreement Template – for Foundation / KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

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

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

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

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

Signed (parent): .....



# Acceptable Use Policy Agreement

## School Policy

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

## Acceptable Use Policy Agreement

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

For my professional and personal safety:

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

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

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

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

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

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

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

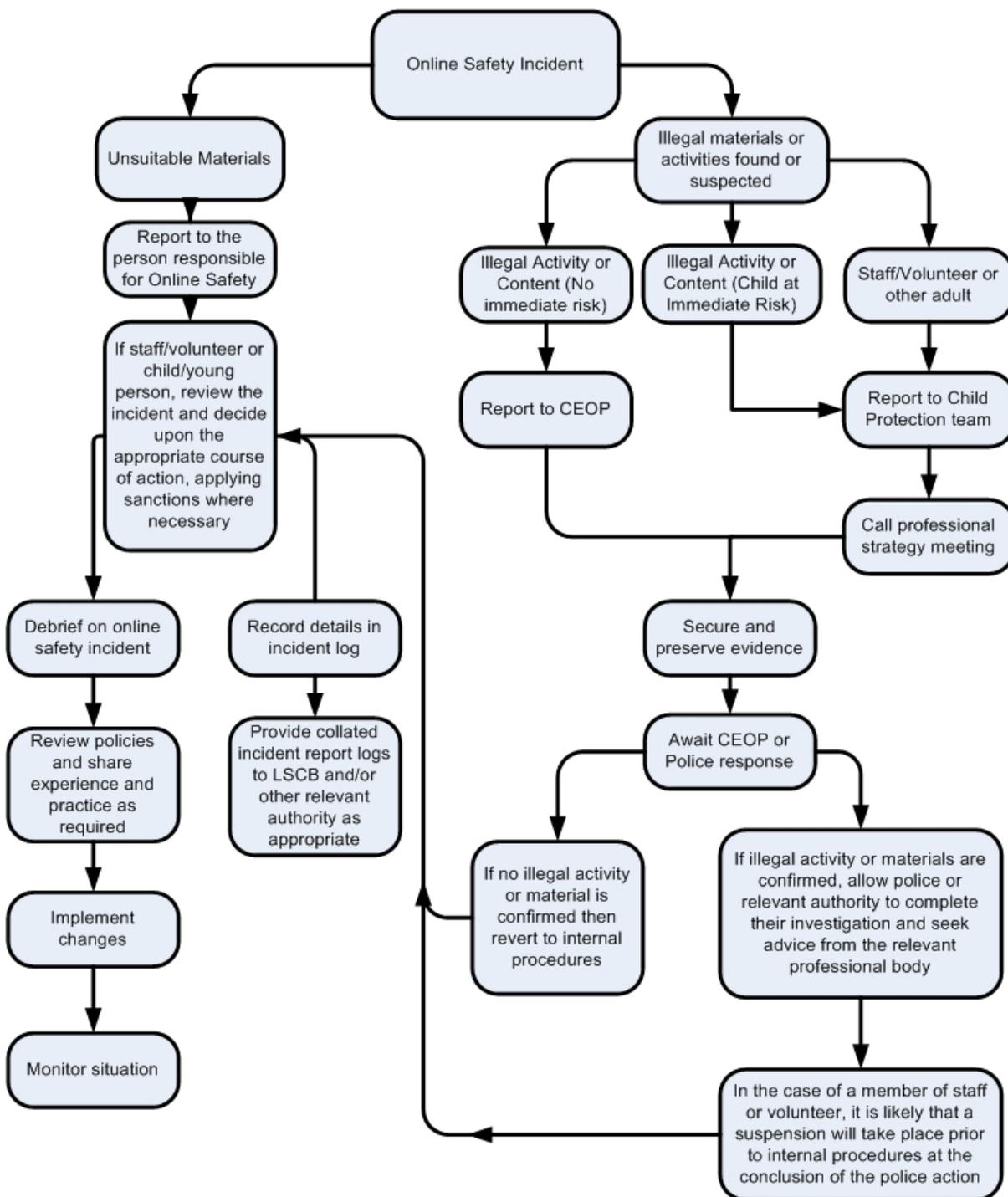
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff or Volunteer Name: .....

Signed: .....

Date: .....

# Responding to incidents of misuse – flow chart







## Monitoring

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

### Audit / Reporting

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

- the second responsible person (Headteacher)
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

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

### Further Guidance

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" ([Revised Prevent Duty Guidance: for England and Wales, 2015](#)).

Furthermore the Department for Education published [proposed changes](#) to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

In response UKSIC produced guidance on – information on "[Appropriate Filtering](#)"

NEN Technical guidance: <http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/>

Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: <https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx>