Simonside Primary School

Online Safety Policy

Introduction

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

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students/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, 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. 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, Amy Thomas, has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- Meetings with the Online Safety lead
- Attendance at Online Safety Group meetings as/when relevant
- Monitoring of online safety incident logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors

Head Teacher and Senior Leaders

- The Head Teacher 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 Lead. At Simonside Primary School the delegated Online Safety Lead is Emma Hills, Deputy Head Teacher.
- The Head Teacher and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head Teacher and Senior Leaders are responsible for ensuring that the Online Safety Lead 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 Head Teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring updates and reports from the Online Safety Lead.

Online Safety Lead

- Takes day to day responsibility for online safety issues.
- Has a leading role in establishing and reviewing the school online safety policies and documents with the Computing Lead.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Works collaboratively alongside the Computing Lead to co-ordinate training and advice for staff, pupils and parents.
- Liaises with the Local Authority and any other relevant bodies.
- Liaises with the school Computing Lead regarding any policy or curriculum updates.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets with Online Safety Governor(s) to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings of Governors.
- Reports regularly to Senior Leadership Team.

Technical Staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any Local Authority or other relevant body guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Technical Staff 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
- The use of the networks including the internet and digital technologies is regularly monitored in order to ensure that any misuse or attempted misuse can be reported to the Head Teacher, Senior Leaders and Online Safety Lead for further investigation.
- 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 online safety policy and practices
- They have read, understood and signed the staff acceptable use policy.
- They report any suspected misuse or problem to the Head Teacher, Senior Leadership Team and/or Online Safety Lead for further investigation and action, when relevant.
- All digital communications with students, pupils, parents and carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the Online Safety Policy and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (when/where relevant) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

The Designated Safeguarding Lead 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
- Online-bullying

Pupils

- Are responsible for using the school's digital technology systems in accordance with the pupil acceptable use agreement.
- Should have a good understanding of research skills. Such level of understanding should be in line with their age/year group Computing curriculum content and expectations.
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on 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 and 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, the school website, social media and the distribution of any further information about national as well as local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and any other Learning Platforms
- Their children's personal devices in the school

In addition to this, parents and carers will be encouraged to support the school in promoting good online safety practice at home and follow guidelines on the appropriate use of:

- The internet
- Gaming, including but not exclusive of, community games
- Social Media, including but not exclusive of, the use of image, video or messaging apps
- The use of any other technologies of which their children have access to
- Reporting any inappropriate or unsafe content or activity

Community Users

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

Education

Pupils

Whilst regulation and technical solutions are very important, such use must be balanced by ensuring appropriate and relevant education of all students encouraging them to take a responsible approach. The education of pupils in online safety and 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. It will be provided in the following ways:

- A planned online safety curriculum as part of Computing, PHSE and other lessons when and where it is relevant.
- Online safety should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside of school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites of which they visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other

relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should however, be auditable, with clear reasons for the need.

Staff and 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:

- Planned online safety training will be made available to staff. This will be regularly updated and reinforced.
- An audit of the online safety training needs of all staff will be carried out annually.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead or Computing Curriculum Lead (Katie Frizzell) will receive regular updates through attendance at external training events 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.
- The Online Safety Lead or Computing Curriculum Lead will provide advice/guidance/training to individuals as required.

Governors

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

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training sessions for staff
- Participation in any relevant training sessions for parents.
- Access to any online training and resources shared through any of the above.

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 online 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, the school website and other Learning Platforms
- Parents/carers sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

The Wider Community

The school will provide opportunities for 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.
- Sharing their online safety expertise and general good practice with other local schools.
- Supporting community groups to enhance their online safety provision when/where relevant.
- Providing family learning updates regarding the use of new digital technologies, digital literacy and online safety.

Technical Support Team

The school will be responsible for ensuring that the school network and general infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users at KS2 will be provided with a username and secure password by the relevant member of staff who will keep an up to date record of users and their usernames.
- Users are responsible for the security of their username and password.
- Group or class logons and passwords for KS1 and below may be chosen to be used for certain programmes.
- The "administrator" passwords for the school systems, used by the Network Manager must also be available to the Head Teacher or other members of the senior leadership team and kept in a secure place.
- Helen Rothbell is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes.

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school provides enhanced/differentiated user-level filtering appropriately
- 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 devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned or 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.

Depending on the allocation and intended use of the device it may have access to the wider internet which could include the school's learning platform and other 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 school acceptable use agreements for staff, students and parents/carers will give consideration to the use of mobile technologies but a general indication of permissions for the use of digital devices is outlined in the table below:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes but must handed in at the office on arrival and collected at the end of the school day. Not permitted for use in school.	Yes	Yes
Full network access	Varies depending on login and assigned permissions	Varies depending on login and assigned permissions.	No	No	No	No
Internet only	Varies depending on the device e.g iPad – internet access, Computer – potential network access.	Varies depending on how the device is set up and the intended use.	Yes	-	Varies depending on assigned permissions.	Varies depending on assigned permissions – nature of visit and purpose of use
No network access	Varies depending on the device e.g iPad -no access, Computer – access.	Varies depending on how the device is set up and the intended use.	No access.	-	-	-

Use of Video and Digital Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks through its Computing and Digital Literacy curriculum and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Written permission from parents or carers will be obtained before photographs of students are published on the school website, social media, local press or any further relevant platforms. Such permissions will be acquired through the completion of the school's Images and Videos Parental Consent Form which is completed as part of the pupil induction process.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school ensures that it:

- Has a Data Protection Policy.
- Implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- Has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- Has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- Has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- Has information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- Will hold only 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.
- Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents and any other appropriate adults with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- Has procedures in place to deal with the individual rights of the data subject.
- Carries our data Protection Impact Assessments (DPIA) are carried out when/where.
- IT system security is ensured and regularly checked. Other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom and to learners
- Has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Provides all staff with data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.

- Device must be password protected.
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, at all times.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school.
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Do not transfer any school personal data to personal devices except as in line with school policy
- Access personal data sources and records 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.

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school's email service to communicate with others when in school or using school systems by remote access.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers 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.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff if/when relevant.

Social Media – Protecting Professional Identity

School have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Therefore, 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 students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school
- 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.
- The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

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
- The school permits reasonable and appropriate access to private social media sites.

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.

Dealing with unsuitable/inappropriate activities

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

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on,	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	

material, remarks, proposals or comments that contain or relate to:	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping/commerce					X	
File sharing					X	
Use of social media					X	
Use of messaging apps					X	

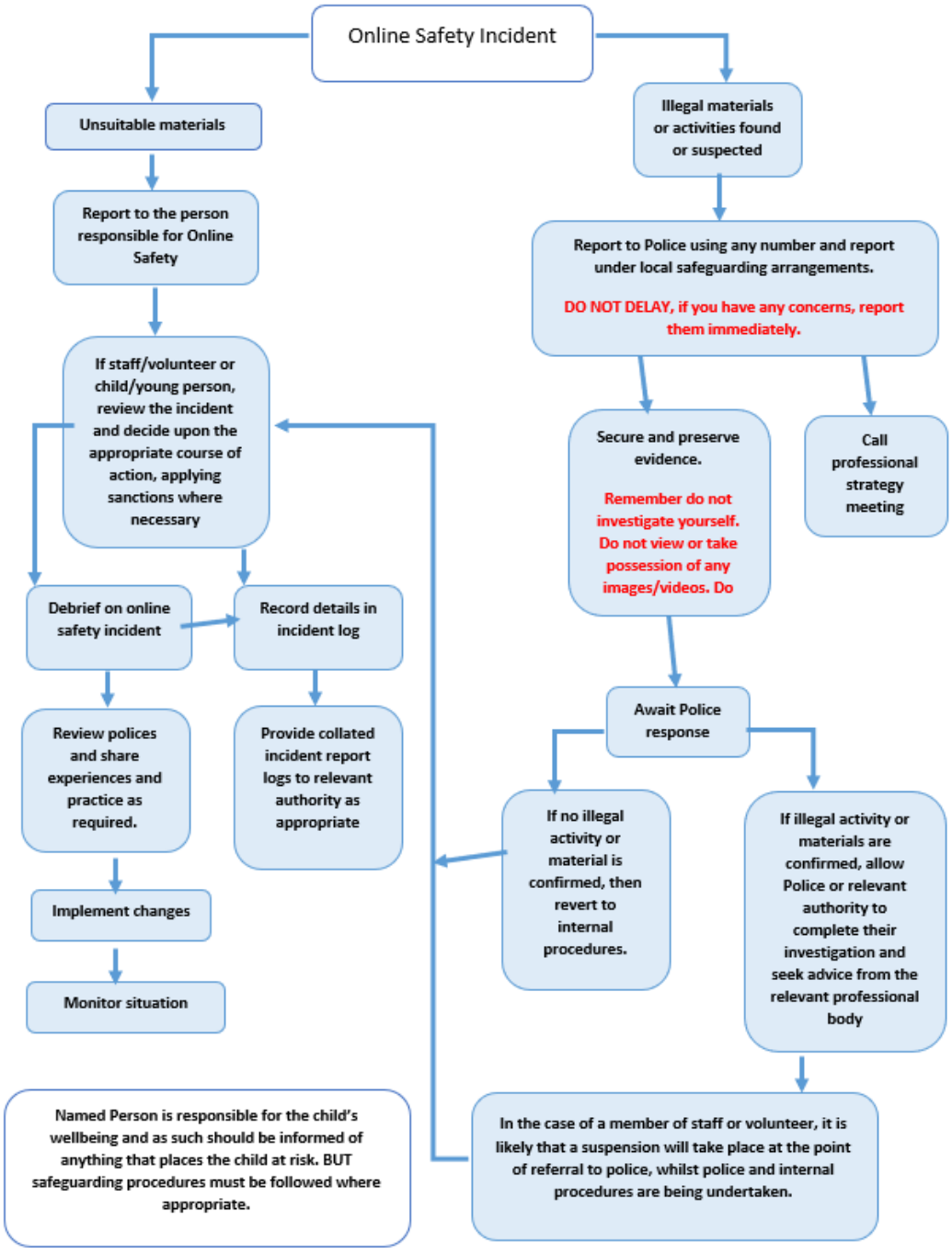
Use of video broadcasting e.g. Youtube					X	

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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 technologies, who understand and follow the 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.

During such instances or in the event of suspicion all steps within this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

Isolate the computer in question as best as you can as 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 and Sanctions

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher	Refer to Head of	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	Warning	Further sanction e.g.
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									
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device									
Unauthorised/inappropriate use of social media/ messaging apps/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school/academy network by sharing username and passwords									
Attempting to access or accessing the school/academy network, using another student's/pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's/academy's filtering system									

Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Actions/Sanctions

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

Actions which could compromise the staff member's professional standing								
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy								
Using proxy sites or other means to subvert the school's/academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Policy updated: February 2022

To be reviewed: February 2023