Digital Safety Policy

Development / Monitoring / Review of this Policy

This Digital Safety policy has been developed by the Digital Safety Group made up of:

- Headteacher/DSL
- Digital Safety Lead
- Computing Lead/Governor
- Digital Safety Governor
- Chair of Governors

Schedule for Development / Monitoring / Review

This Digital Safety policy was approved by the Governing Body.	Summer 2018
The implementation of this Digital Safety policy will be monitored by the:	Digital Safety Group Senior Leadership Team
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the Digital Safety policy generated by the monitoring group (which will include anonymous details of Digital Safety incidents) at regular intervals:	Once a year
The Digital 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 Digital Safety or incidents that have taken place. The next anticipated review date will be:	Summer 2019
Should serious Digital Safety incidents take place, the following external persons / agencies should be informed:	Designated Safeguarding Lead Police/CSC/External agencies Headteacher Chair of Governors

The school will monitor the impact of the policy using:

- Logs of reported incidents and feedback from staff, parents and pupils.

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 and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Digital 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 Digital Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the Digital Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Digital Safety incidents and verbal monitoring reports. A member of the Governing Body has taken on the role of Digital Safety Governor. The role of the Digital Safety Governor will include:

- regular meetings with the Digital Safety Co-ordinator
- regular monitoring of Digital Safety incident logs
- reporting to BSPM committee.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including Digital Safety) of members of the school community, though the day to day responsibility for Digital Safety will be delegated to the Digital Safety Co-ordinator.
- The Headteacher and DSL should be aware of the procedures to be followed in the event of a serious Digital Safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Digital Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Digital Safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will support those in school who carry out the internal Digital 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 termly monitoring reports from the Digital Safety Co-ordinator.

Digital Safety Coordinator:

The Digital Safety Co-ordinator is Miss Charlotte Bowker for the academic year 2018/2019.
The Digital Safety Co-ordinator will -

- lead the Digital Safety committee
- take day to day responsibility for Digital Safety issues and has a leading role in establishing and reviewing the school Digital Safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of a Digital Safety incident taking place
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of Digital Safety incidents and creates a log of incidents to inform future Digital Safety developments.
- meet termly with the Digital Safety Governor to discuss current issues, review incident logs and filtering / change control logs – this will help direct the agendas of the termly Digital Safety Group meetings.
- attend relevant meetings
- report termly to the Senior Leadership Team.

Network Manager

The Digital Safety Network Manager is currently BT Lancashire Services for the academic year 2018/2019.
The Digital Safety Network Manager will ensure-

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Digital Safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed annually
- that they keep up to date with Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant
- that the use of the network / internet is monitored half termly in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Digital Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are kept functional and up to date.

Teaching and Support Staff

The teaching and support staff are responsible for ensuring that:
- they have an up to date awareness of Digital Safety matters and of the current school Digital Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Digital Safety Coordinator / Senior Leader / Headteacher / for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Digital Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Digital Safety and acceptable use policies
- Pupils have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

The DSL is Lisa Gaskell (back up Joanne Curran) for the academic year 2018/2019.

The DSL should be trained in Digital 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.

Digital Safety Group

The Digital Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Digital Safety and the monitoring the Digital Safety policy including the impact of initiatives. The group will also be responsible for termly reporting to the Governing Body.

Members of the Digital Safety Group will assist the Digital Safety Coordinator with:
- the production / review / monitoring of the school Digital Safety policy / documents
- monitoring and reviewing the Digital Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the Digital Safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Currently this group consists of Charlotte Bowker, Chris Mitchell, Elaine Lambert, Greg Fedun, Pat Jones, Lisa Gaskell.

Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy / Digital Safety Code of Conduct
- have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Digital Safety practice when using digital technologies out of school and realise that the school's Digital 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 / local Digital Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Digital Safety practice and to follow school guidelines on the appropriate use of:
- digital and video images taken at school events
- their children's personal devices at home.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Digital Safety is therefore an essential part of the school's Digital Safety provision. Children and young people need the help and support of the school to recognise and avoid Digital Safety risks and build their resilience.

Digital Safety should be a focus in all areas of the curriculum and staff should reinforce Digital Safety messages across the curriculum. The Digital Safety Curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned Digital Safety curriculum is provided as part of Computing / PHSE / other lessons (we currently use the Lancashire Curriculum as a back bone for this).
- Key Digital Safety messages are reinforced as part of a planned programme of assemblies.

- Pupils are taught to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to respect copyright when using material is accessed on the internet.
- Pupils will 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 will 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 will 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 will 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 Digital 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 eg Safer Internet Day
- Reference to the relevant websites.

Education & Training – Staff / Volunteers

It is essential that all staff receive Digital Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- This Digital Safety policy and its updates will be presented to and discussed by staff.
- The Digital Safety Coordinator will provide advice / guidance / training to individuals as required.
- The Digital Safety Coordinator and DSL will receive regular updates through attendance at external training events.
- All new staff should receive Digital Safety training as part of their induction programme, ensuring that they fully understand the school Digital Safety policy and Acceptable Use Agreements.

Training – Governors

Governors will be encouraged to take part in Digital Safety training / awareness sessions,

This may be offered in a number of ways:
- Attendance at training provided by the Local Authority / National Governors.
- Regular opportunities will be provided for school based training / parents or staff information sessions.

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 Digital Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews 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 will be provided with a username and secure password by school technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- Internet access is filtered for all users by the Lightspeed Filtering System provided by BT Lancashire. 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 by Lightspeed Filtering System provided by BT Lancashire and internet use is logged and regularly monitored. There is a clear process in place, by the Lightspeed Filtering System provided by BT Lancashire to deal with requests for filtering changes.
- The school has provided differentiated user-level filtering for pupils and staff.
- 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 by BT Lancashire 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.
- At the discretion of the head teacher guests to school eg trainee teachers and supply teachers may be provided with temporary access onto the school systems.
- The extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school is detailed later in this policy.

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 / 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other 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 students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Student's / Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are identified
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are procedures for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:
- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

Communication Technologies / User Actions	Staff and other Adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school (Staff and Year Six)	✖				✖			
Mobile phones in school – EYFS/Yr1/Yr2/Yr3/Yr4/Yr5								✖
Use of mobile phones in lessons				✖				✖
Use of mobile phones in social time		✖						✖
Taking photos on mobile phones / cameras				✖				✖
Use of other mobile devices eg tablets, gaming devices		✖				✖		
Use of personal email addresses in school, or on school network				✖				✖
Use of school email for personal emails				✖				✖
Use of messaging apps		✖						✖
Use of personal social media				✖				✖
Use of personal blogs				✖				✖
Use of personal video broadcasting (eg Youtube)				✖				✖
Online gaming (educational)		✖				✖		
Online gaming (non-educational)		✖				✖		
Online gambling				✖				✖
Online shopping/commerce		✖						✖

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

- The official school email service may be regarded as safe, secure and monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE 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.
- Currently pupils access email services only through the walled-garden within the Purple Mash Service.
- Pupils should be taught about Digital 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.

Mobile Phones

Mobile phones may be brought into school by staff and Year Six children only.

- Staff can use their mobile phones during breaks, away from the children (unless awaiting an emergency call).
- Year Six children store their phones in a draw in Year Six and collect them at the end of the day. A letter goes out to children in their last term of Year Five outlining the rules of bringing a mobile phone into school. The mobile phones are not locked away and the school is not liable for any broken or lost mobile phones in Year Six. Year Five/Six parents sign a document to agree to these terms.

iPads

- All staff and children must use the school iPads when on the school grounds. Personal iPads are not to be brought into school.

Twitter

Penwortham Primary School is looking towards developing an online blogging presence via Twitter within the next three years. Any content that is posted will be strictly school related. Children's photographs, videos and images will only be published with consent of the child's parents. Any staff photographs, videos and images will only be published with consent of the staff member. The policy will be updated when this happens.

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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority

- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Senior Leadership Team.

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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						X
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
Use of video broadcasting eg Youtube					X	

Responding to incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.
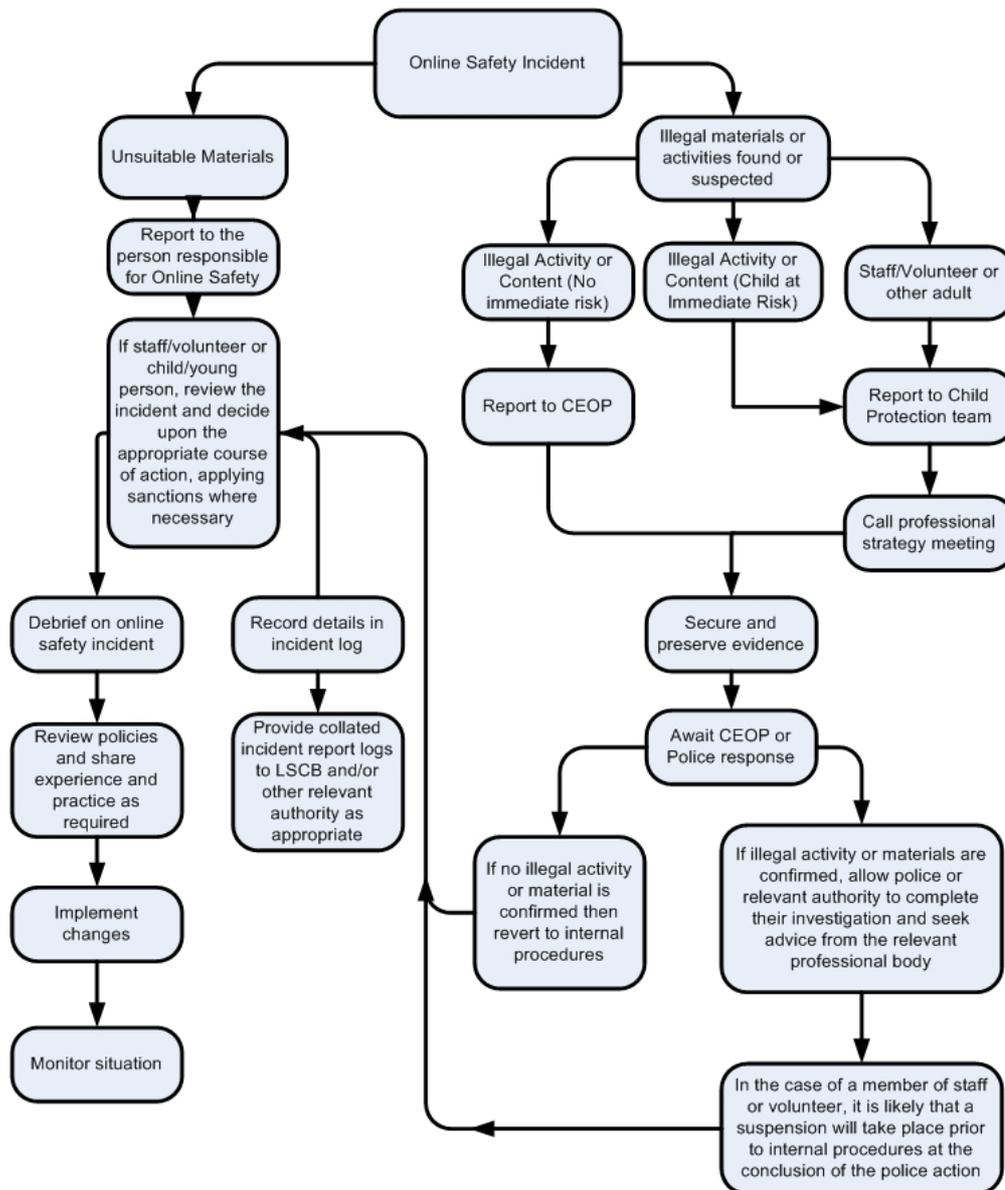
Other Serious Incidents

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
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

Students / Pupils   Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Department	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	X		X	X		X
Unauthorised use of non-educational sites during lessons	X					X			
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X			
Unauthorised use of social media / messaging apps / personal email	X		X			X	X		
Unauthorised downloading or uploading of files	X	X	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				
Attempting to access or accessing the school / academy network, using the account of a member of staff		X	X		X	X	X	X	X
Corrupting or destroying the data of other users		X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X	X
Using proxy sites or other means to subvert the school's / academy's filtering system			X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X		X

Staff
Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email		X	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X	X	X	X		
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	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 / academy	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions			X	X			X	X