



# Pencalenick School

## Online Safety Policy

Updated May 2018



**SPECIAL PARTNERSHIP TRUST**

An Ambitious, Inspirational Partnership of Outstanding Learning

# Development, monitoring and review of this policy

This Online Safety policy has been developed by the e-Safety group made up of:

- Head of School
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Local Governing Board
- Members of the SPT trustees

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

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head of Schools / Principals 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. 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:

## Local Governing Body (LGB):

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 LGB who receiving regular information about online safety incidents and monitoring reports.

A member of the LGB has taken on the role of Online Safety Governor.

The role of the Online Safety Governor includes:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs as part of the termly safeguarding report
- regular monitoring of filtering / change control logs which will inform the safeguarding report.
- reporting to relevant Governors / Board / Committee / meeting

## Head of School and Senior Leaders:

- The Head of School 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 supported by Future Clouds and the , and the Designated Safeguarding Leads (DSLs).
- The Head of School and the Head of Care and the Assistant Heads are 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 Head of School / 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 Head of School / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- In the case of a serious breach of online safety Visigo operatives will notify the DSLs and the Online Safety Coordinator within 15 minutes of the incident. Appropriate action will be taken according to safeguarding procedures.

## 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 / Director to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
- provide parent workshops on internet safety and aid parents to understand the Acceptable Use Policy.
- Regularly update information on the school website.

## Network Manager:

The Network Manager is 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 requirements may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School / Senior Leader; Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in the SPT policies

## Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Head of School / Senior Leader ; Online Safety Coordinator 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**
- 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 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
- will be responsible for aiding the pupils to understand the Acceptable Use Agreement.

## 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
- 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 / Directors.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator (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 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 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 Student / Pupil Acceptable Use Agreement and will be assisted to do this according to their cognitive ability.**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- pupils will be assisted to change their passwords each term.

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and

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

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

## Community Users

Community Users login and out of the office this means that they agree to follow protocols regarding internet use and the use of digital technology whilst on the premises. Social events and parents evenings will be carefully monitored by school staff and where possible parents will be asked to register.

# 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 throughout the child's time in school.**
- **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 by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- **Internet safety day will be followed annually.**
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff 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. Visigo will assist in the monitoring of this.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit. This is supported by Visigo.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

## Education – The Wider Community

The school will provide opportunities for community who are associated with Pencalenick to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups when requested inline with our policy on outreach work.

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:

- **Formal online safety training is completed by staff annually as part of the safeguarding programme. Regular updates will be given as new directives are produced. An audit of the online safety training needs of all staff will be carried out regularly by the DSL.**
- **All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- Online safety as a training need will be identified through appraisals and within the performance management process.
- The Online Safety Coordinator and DSLs 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.
- The Online Safety Coordinator /DSL will provide advice / guidance / training to individuals as required.

## Training – Governors

**Governors will 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 & safety and safeguarding. This may be offered in a number of ways:

- Attendance at training events outside school.
- Participation in school training and information sessions for staff or parents

## Technical – infrastructure, equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users have clearly defined access rights to school technical systems and devices.**
- **All staff are issued with a username and then be expected to devise a secure password which they will be instructed to change every 90 days. Users are responsible for the security of their username and password.** All pupils shall have a user name provided by the network manager and will be assisted to create a password which they will change termly depending on their cognitive ability.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Head of School or other nominated senior leader and kept in a secure place (e.g. 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
- **Internet access is filtered for all users.** Illegal content 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 by Visigo. There is a clear process in place to deal with requests for filtering changes through subject coordinators, tutors, Head of Care and DSL.
- **Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.**
- The school has provided enhanced or differentiated user-level filtering allowing different filtering levels for staff
- Users are made aware that systems may be monitored
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the DSL and Online Safety Coordinator.

- 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.
- School Mobile devices will not be used by family members and the AUP will be adhered to by staff even when offsite.
- Staff are permitted to download executable files and apps on school devices that are appropriate to their work.
- Information and documents is stored on password protected removable media (eg memory sticks, hard drives and I pads / tablets) 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 Bring Your Own Device /Technology)

Mobile technology devices may be school owned 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 and therefore must adhere to this policy, the Staff Code of Conduct and Safeguarding Protocols.

## Use of digital and video images

Staff, parents / carers and pupils are aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement strategies to reduce the likelihood of the potential for harm:

- **When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they 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**
- 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 or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital and video images.

- Staff and volunteers are allowed to take digital and 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 and 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.

## 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)**
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

**Staff must ensure that they:**

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

When personal data is stored on any portable computer system, memory stick or any other removable media:

- **the data must be encrypted and password protected**
- **the device must be password protected**
- **the device must offer approved virus and malware checking software**
- **the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete**

## **Social Media - Protecting Professional Identity**

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
- As part of this policy and the code of conduct there is a clear 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 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 will be taken
- The school permits reasonable and appropriate access to private social media sites for staff.

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 the Online Safety Group to ensure compliance with the school policies.

## 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, 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 safeguards employed by the school				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		

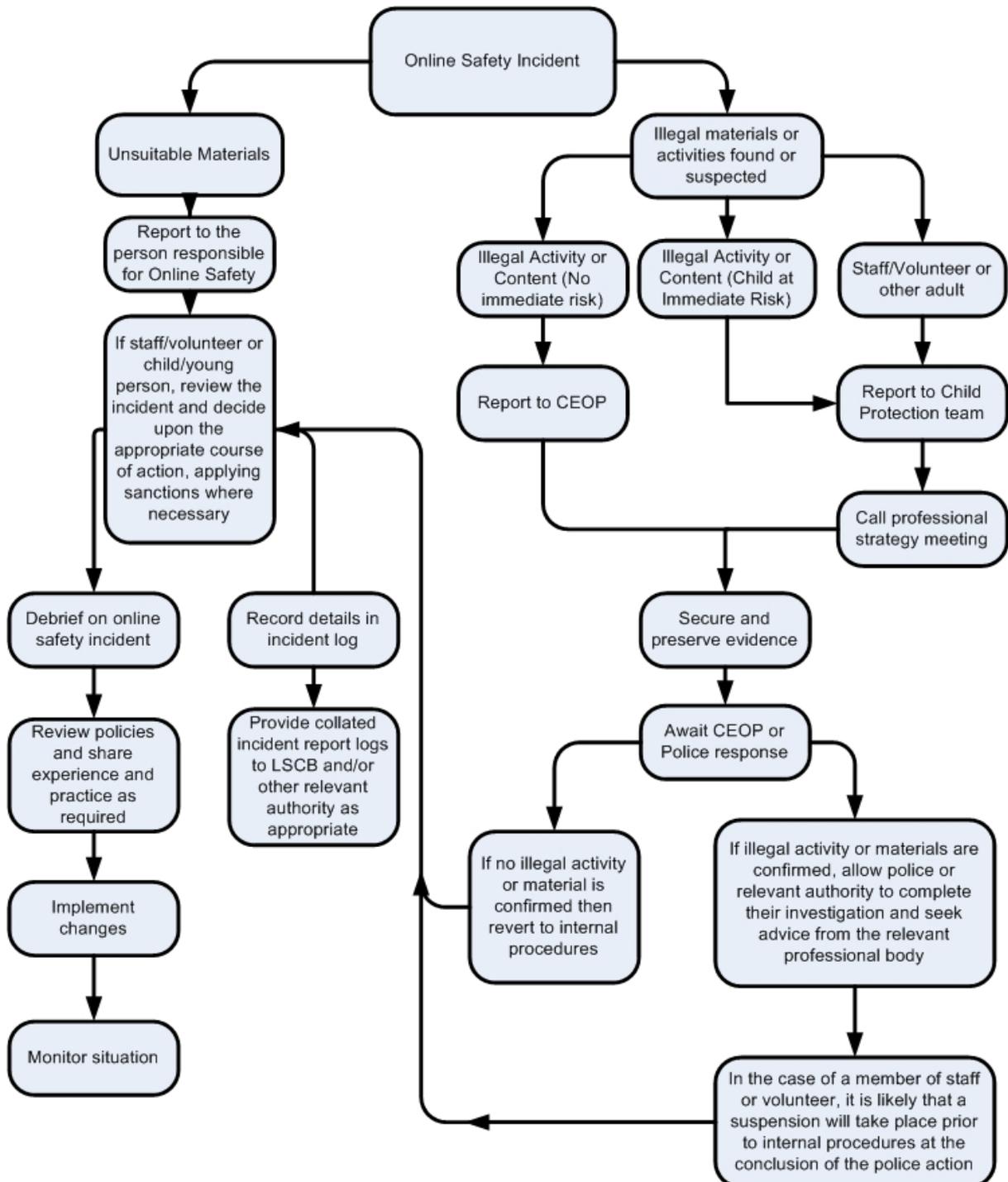
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

## Responding to incidents of misuse

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

# Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (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 / 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
  - 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:

Pupils Incidents	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Designated Safeguarding Lead	Refer to Head of School	Refer to Police	Refer to NM 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		X
Unauthorised use of non-educational sites during lessons	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	X	X		
Unauthorised downloading or uploading of files		X	X		X	X	X		
Allowing others to access school network by sharing username and passwords		X	X		X	X	X		X
Attempting to access or accessing the school network, using another student's / pupil's account		X	X		X	X	X		X
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X	X	X		X

Corrupting or destroying the data of other users									
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		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X		X
Using proxy sites or other means to subvert the school's / 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	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X			X		X	
	<b>Actions / Sanctions</b>								
<b>Staff Incidents</b>									
	Refer to line manager	Refer to Head of School	Refer to Local Authority / HR	Refer to Police	Refer to NIM 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					X
Inappropriate personal use of the internet / social media / personal email		X			X	X			
Unauthorised downloading or uploading of files	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
Careless use of personal data e.g. holding or transferring data in an insecure manner						X			x
Deliberate actions to breach data protection or network security rules		X	X	X					X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									x
Using personal email / social networking / instant messaging /									

text messaging to carrying out digital communications with pupils		X	X					X
Actions which could compromise the staff member's professional standing		X			X	X		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		x
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X					X
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

# Appendices

Responding to incidents of misuse – flow chart

Online Safety Flowchart for pupils - Please see on our website

# Responding to incidents of misuse – flow chart

