



# Perranporth School Online Safety Policy

Revised June 2021

## Perranporth Online Safety Policy

### Development / Monitoring / Review of this Policy

This Online Safety Policy has been developed by Perranporth Primary School safeguarding committee made up of:

- Computing and Online Safety Coordinator
- Head teacher / Safeguarding Governor
- Health and Safety Officer/ Governor
- Staff – including Teachers, Support Staff,
- Technical Staff - ICT4
- School Council, Digital Leaders and Diamond 6 Pupils

### Schedule for Development / Review

The policy has been reviewed to reflect **PREVENT** training, Promoting British values and SMSC.

Mrs Barrett (School Business Manager) will inform the Governing Body when necessary, of any significant online safety incidents. Mrs Barrett receives and monitors filtering alerts in real time on a daily basis.

The Online Safety Policy is reviewed regularly, in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Should serious online safety incidents take place, the following external persons / agencies should be informed:

**Cornwall Police, CEOP and/or IWF**

The school will monitor the impact of the policy using:

- ✓ *Logs of reported incidents*
- ✓ *Monitoring logs of internet activity (including sites visited)*
- ✓ Formal and informal assessment of children's understanding of E-safety through classroom practise and the computing curriculum delivery.

### 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 Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour and Safeguarding policies.

The school will deal with such incidents within this policy and associated Safeguarding, Behaviour and Anti-Bullying policies and will inform parents / carers of incidents of inappropriate online safety behaviour that took 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.

## Headteacher and Senior Leaders:

- ✓ The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, however, the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator and Class Teachers.
- ✓ The Headteacher and the Deputy Head Teacher 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 Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- ✓ The Headteacher 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.

## Online Safety Coordinators:

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents / current filtering lists
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with ICT4 for filtering requirements and monitoring
- liaises with school staff on current issues and updates
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- reports regularly to Senior Leadership Team

## Network Manager: ICT4

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 GDPR regulations and any new TPAT academy requirements / other relevant body online safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed (teaching Staff)
- 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 / virtual learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Coordinator / for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

## Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices, provided by termly briefings from Esafetysupport.com
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement
- they report any suspected misuse or problem to the Headteacher; Online Safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- **online safety awareness is embedded in all aspects of the curriculum and other activities**
- students / pupils understand and follow the online safety rules and acceptable use policy guidance.
- students / 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 be aware of the reporting processes in place for dealing with any unsuitable material that is found in internet searches
- they have undertaken or are aware of **KCSE** (Safeguarding update Sept 2018)\_CSE (Child Sexual Exploitation)\_ and **PREVENT** training and know which signs to look out for in cases of radicalisation.

Teaching staff should be aware that children who **have not** followed school rules/protocol and handed in mobile devices at the school office on entry to school, may be able to bypass school filters by using 3G or 4G capability on personal devices.

#### Lead Safeguarding Officer: Mr A Johnson

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
- any forms of radicalisation
- any form of child sexual exploitation

#### Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- will be taught research skills and the need to avoid plagiarism and uphold copyright regulations
- will 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 rules on the use of mobile devices, including all phones and other devices with 3G and 4G capabilities being left at the school office on arrival to school and only collected at the end of the day.
- should know and understand rules on the taking / use of images and on cyberbullying.
- 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.
- will receive regular planned online safety lessons as well as cross curricular links to staying safe online

- will have read and signed a yearly update of the Pupil Code of Conduct for their age/year group and uphold these rules when using internet systems in and out of school.

### Parents / Carers

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

- digital and video images taken at school events
- their children's personal devices in the school
- access to parents' sections of the website and use of the learning platform to read important online safety advice and updates.

The school will support parents by offering regular briefings including information on **CSE, PREVENT**, signs of online grooming, monitoring new technology and acceptable use. Termly online training modules provided by E-safetysupport.com are emailed to our parents and signposted from our website.

### Policy Statements

#### Education – students / 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 Perranporth School's online safety provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

All teaching staff are trained in **Safeguarding, CSE & PREVENT** and are responsible for teaching this primarily as part of **Promoting British Values, Spiritual, Moral, Social and Cultural education** and the **Computing Curriculum** but also through the broader curriculum wherever relevant. (The Prevent strategy is the Government's response to help counter the extreme ideologies that recruit **vulnerable people** and to offer guidance and support to those who are drawn to them. Much of the work is dominated by the opposing ideologies of far-right extremism (neo-Nazi) and violent Islamists (Al Qaeda, ISIS), although the strategy addresses all forms of extremism. Local delivery of Prevent is aligned with Community Safety and Safeguarding; **all communities are affected by violent extremism** and those most vulnerable to the ideologies are the young, particularly through the use of the internet.

Online safety should be a focus across all areas of the curriculum and staff should reinforce online safety messages across the broader curriculum. The online safety curriculum has been developed and adapted using a combination of Rising Stars, E-safetySupport.com and Inspire and is a broad and relevant curriculum that has clear progression, with opportunities for creative activities linked to PBV and SMSC education (See appendices).

These will be provided in the following ways:

- **A planned online safety curriculum is provided as part of Computing but also features in / PHSE / SMSC, PBV and other cross curricular lessons and should be revisited in each Computing unit of work**
- **Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- Pupils are helped to understand the need for the relevant age appropriate Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- Staff must act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics 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:

- online safety support parents modules (we are subscribed to training from e-safetysupport.com)
- Curriculum activities / homework
- Letters, newsletters, web site
- Parents / Carers online safety sessions with local police attendance
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg [www.swgfl.org.uk](http://www.swgfl.org.uk)  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>  
<https://ceop.police.uk/> <http://www.kidsmart.org.uk/> <https://www.thinkuknow.co.uk/>

### Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- **A planned programme of formal 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 regularly.**
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the schools online safety policy and Acceptable Use Agreements.**
- The Online Safety Coordinator 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 meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.
- Safeguarding PREVENT and CEOP Training for all staff



## Training – Governors / Directors

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

- Attendance at training provided by the TPAT Academy group
- E-safety Support (subscribed online training and update modules emailed termly)
- Participation in school training / information sessions for staff or parents

## Technical – infrastructure / equipment, filtering and monitoring - Provided by ICT4

ICT4 along with Perranporth School is 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 ensure that the ICT4 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.
- The “administrator” passwords for the school ICT system, used by the Network Manager and Computing Coordinator must also be available to the Headteacher.
- Technical Support Assistant 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 filtering provider (ICT4) by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Agreed sites can be added or removed by Mrs A Barrett or ICT4
- 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
- Potential technical incident / security breaches to be reported in the Online Safety log, in the meeting room.
- 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.  
The school infrastructure and individual workstations are protected by up to date virus software.  
Limited access is in place for guests which includes relevant filtering
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be taken off the school site unless safely encrypted or otherwise secured. All staff laptops are encrypted and staff are provided with encrypted memory sticks for any personal data.
- That the school digital infrastructure and filtering system is compliant with new GDPR regulations.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil's 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. 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, **these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.**
- Staff and volunteers (who have read and signed the relevant staff / volunteer photo/video agreement forms) 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 where possible always be taken on school equipment**. If school equipment is not available, then permission **must be obtained** for the use of personal equipment AND any images should **only be stored on the school network and removed from personal devices before leaving the premises.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully ensuring that children without photo agreement are NOT included and any written description will only ever include first names.
- 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 or elsewhere.

### Data Protection

Personal data will be recorded, processed, transferred and made available according to the The EU General Data Protection Regulation (GDPR)

- 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 appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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 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 encrypted 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 only (All teachers have encrypted laptops an encrypted memory sticks for use outside of school).**
- **That personal data shared via email is through the Egress encrypted mail.**

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 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:

	Staff & 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
<b>Communication Technologies</b>								
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons		✓		✓				
Use of mobile phones in social time	✓			✓				
Taking photos on mobile phones / 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 social media		✓		✓				
Use of blogs	✓					✓		

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school 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.**
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

#### Social Media - Protecting Professional Identity

All schools 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,

School staff should ensure that:

- No reference should be made in personal 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 / academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video 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 school or outside school when



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

## User Actions

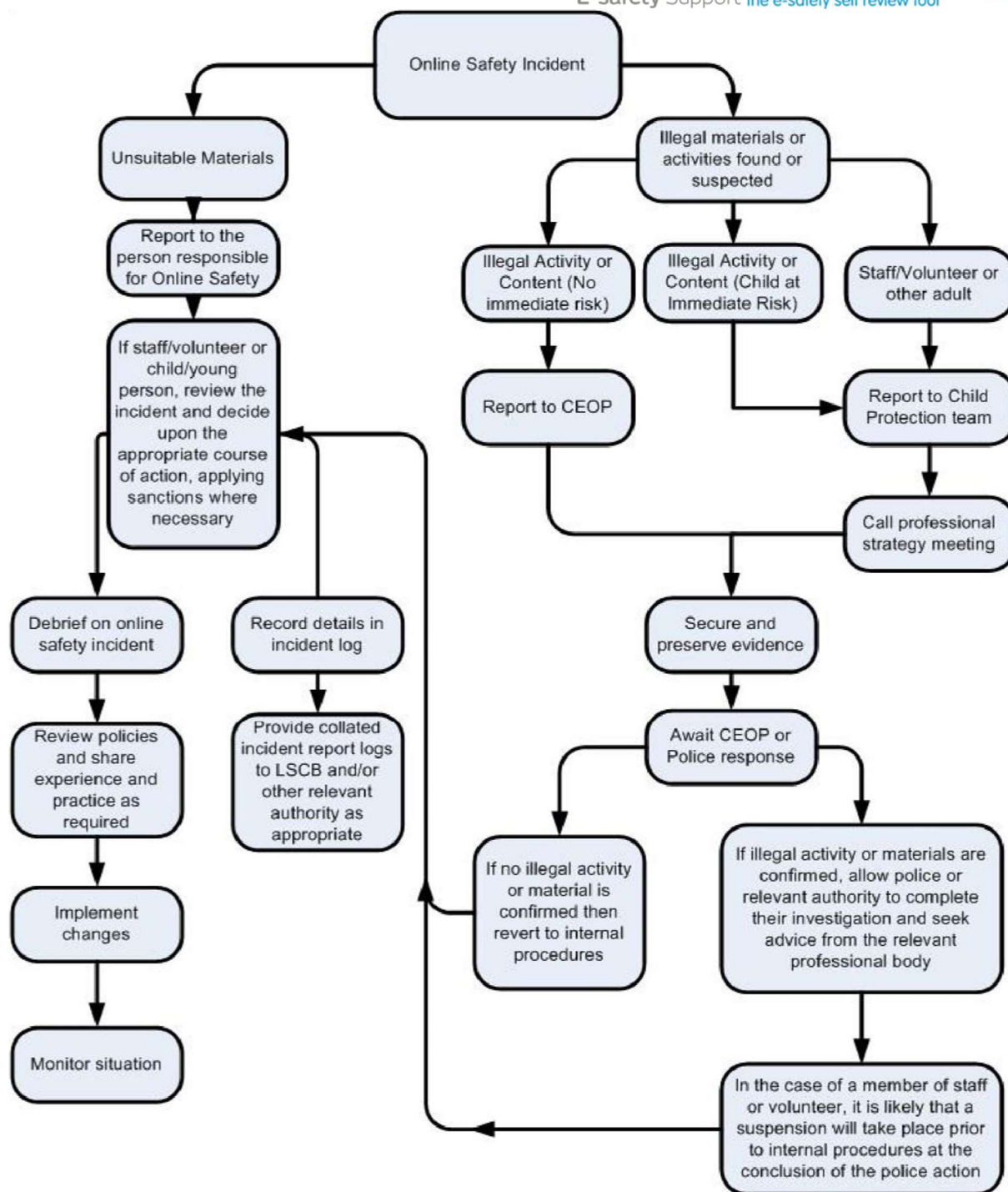
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</b>	Child sexual 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)			✓			
On-line gaming (non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce			✓			
File sharing			✓			
Use of social media			✓			
Use of messaging apps			✓			
Use of video broadcasting eg Youtube			✓			

### 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 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 **see Behaviour Policy**

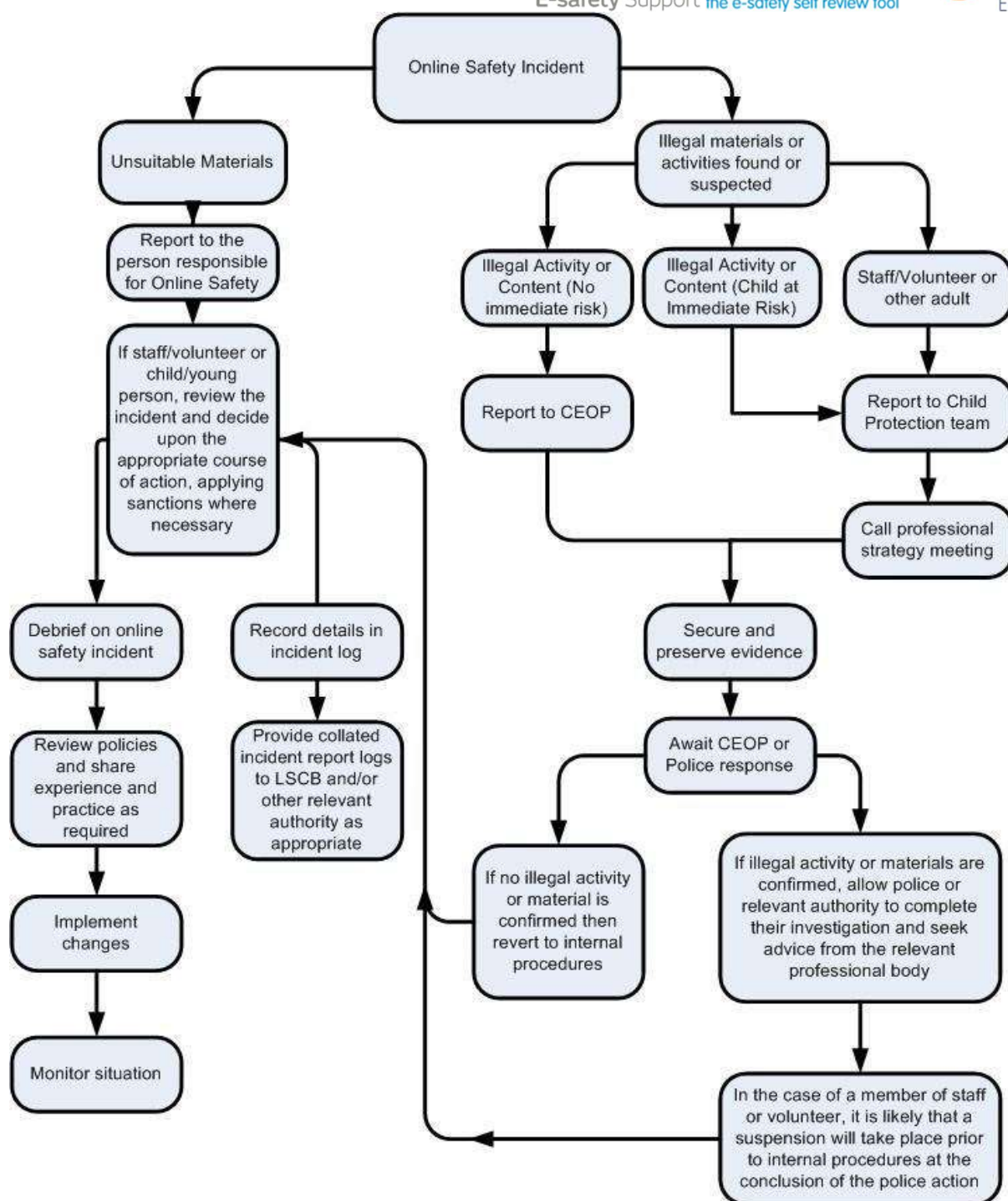




## Staff

## Actions / Sanctions

Incidents:	Refer to line manager	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X				
Inappropriate personal use of the internet / social media / personal email		✓						
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 eg 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		✓	✓	✓				



Reporting Log .....

Group .....

## Training Needs Audit

Training Needs Audit Log Group .... Date .....		Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family online safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol