



Policy for Online Safety

Document Ref: SWAN/IT/POL/27-02-19/90

Name and Title of Author:

Sally Patrick

Name of Responsible

Committee:

Trade Union Representative

Approval:

Implementation Date: January
2019

Review Date: March 2022

Version: 3

Trustee Approval Date:

Target Audience: Staff and
Governors

Related Documents:

Computing Policy, Social Media
Policy, Acceptable Use Policies
(pupils/staff/parents), Anti-
Bullying Policy (Cyber Bullying),
School Technical Security
Policy

References:

Revision History

Version	Date	Summary of Revision	Revision Author
2	Jan 2020	Policy checked against Current Govt Guidance	SP
3	Oct 2020	As above and in light of COVID guidance	SP

Introduction

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

Online safety can be categorised into 3 areas of risk.

Content: being exposed to illegal, inappropriate or harmful material: for example pornography, fake news, racist or radical and extremist views.

Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults.

Conduct: personal online behaviour that increases the likelihood of, or causes of harm; for example making, sending and receiving explicit images, or online bullying.

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, student teachers, visitors,) who have access to and are users of school IT systems, both in and out of the 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. The role of the Online Safety Governor (see website) will include:

- meetings with the Online Safety Leader/Computing Leader (see e-safety web page)
- attendance at Online Safety Group meetings
- monitoring of online safety incident logs
- reporting to relevant Governors at meetings

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see online safety incidents flow chart)
- The Headteacher is responsible for ensuring that the Online Safety Leader 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leader.

Online Safety Leader:

- 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
- liaises with school technical support (One Point)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets with Online Safety Governor to discuss current issues, review incident logs and filtering
- reports regularly to Senior Leadership Team

Network Manager/Technical Support (One Point):

One Point 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 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
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse can be reported to the Headteacher and Online Safety Leader for investigation / action / sanction. This is accessed through the Smoothwall reporting portal.
- that monitoring software/systems are implemented and updated.

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, which includes online abuse, cyberbullying, sexting, upskirting
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher and Online Safety Leader 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
- 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
- there are regular opportunities to teach safeguarding, including online safety. Using resources from
- Have read and adhere to the AUP for working from home (due to Lockdown and/or Bubble bursting)

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOP's advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainst hate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
The use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: <ul style="list-style-type: none"> • Sexting advice; • Online safety: Questions for Governing Bodies; • Education for a connected world framework.
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
igfl	Advice and resources from the London Grid for Learning

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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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
- understand and adhere to the schools AUP when working from home (due to Lockdown/Bubbles burst)

Parents / Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, letters, school website and Twitter updates/alerts. 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 images and videos taken at school events
- their children's personal devices in the school, (where this is allowed)

If children have to work from home parents understand and adhere to the schools AUP when working from home (due to Lockdown/Bubbles burst) and support children as necessary with online learning

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 the school's online safety provision. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/ other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line.
- 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.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents / Carers

Some parents and carers may have 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 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, Twitter alerts/updates
- 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
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> all of which can be found on our school website.

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:

- Online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff will receive online safety training, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Leader and Headteacher will provide advice / guidance / training to individuals as required.

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. One Point will support the school with meeting the above. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (from Reception and above) will be provided with a username and will be asked to set a secure password. Users are responsible for the security of their username and password.
- One Point are 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.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning. 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media.
- 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 pupils in the digital / video images.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used on the school website or Twitter when in association with photographs

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Please see the following table for permissions:

	<i>Staff & other adults</i>				<i>Pupils</i>			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies <i>(within school hours)</i>								
Mobile phones may be brought to the school	.						.	
Use of mobile phones in lessons				.				.
Use of mobile phones in social time	.							.
Taking photos on mobile phones				.				.
Use of other mobile devices e.g. tablets		.					.	
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:

Users must immediately report 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, Twitter, blogs, Seesaw, Microsoft Teams 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 other social media (including WhatsApp) must not be used for these communications.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Unsuitable / inappropriate activities

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

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

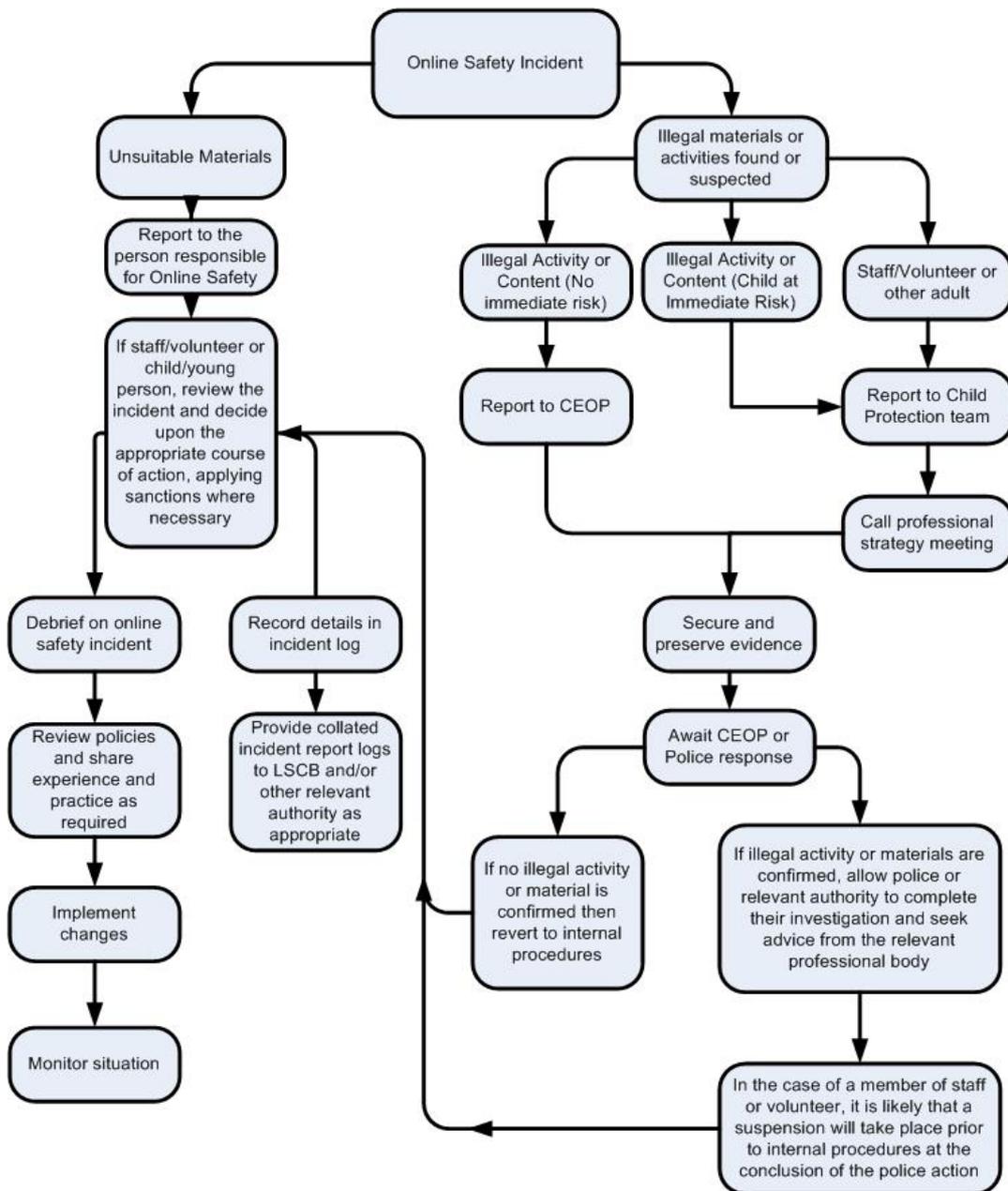
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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		

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

The school may 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.

Digital Technologies Reporting Log

<i>Date</i>	<i>Time</i>	<i>Incident</i> <i>(Include names and specific websites/apps/software/hardware etc)</i>	<i>Action Taken</i>		<i>Incident Reported By</i> (Name and Signature)
			<i>What?</i>	<i>By Whom?</i>	

Appendix – Reporting Log