Rosemellin C.P School

Responsibility: N Finn & P Glover

School Year: 2021/2022

1. 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. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce

these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of the policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

3. Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the *Governing Body on:*	*Summer 2013*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Co-ordinators: Phil Glover & Nicki Finn*
Monitoring will take place at regular intervals:	*Ongoing*
The *Governing Body* will receive an annual report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents).	*Summer term*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	*Summer 2020*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*MAT IT Manager, MAT Safeguarding Officer, Police*

4. Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety 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 when receiving information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator / Officer / Online Safety committee
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible 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-ordinators.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinators and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher / 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.
- The Senior Leadership Team will receive monitoring reports from the Online Safety Co-ordinators.
- The Headteacher and 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 SWGfL flow chart on dealing with Online Safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

Online Safety Coordinators :

- leads the Online Safety committee
- takes day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the school Online Safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- meet with the Online Safety Governor / Online Safety committee to discuss current issues, review incident logs and filtering / change control logs
- attend relevant Governors meetings
- report to the Senior Leadership Team

Network Manager / Technical staff:

The Network Manager and Computing Lead are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Netsweeper is informed of issues relating to the filtering applied by their onsite system
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinators
- that monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinators for investigation
- digital communications with pupils (Virtual Learning Environment (VLE)) 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 school activities
- pupils understand and follow the school Online Safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of devices in lessons, extra curricular and extended school activities
- they are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection / Child Protection Officer

should be trained in Online Safety issues and be aware of the potential for serious child protection 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 Committee

Members of the Online Safety committee will assist the Online Safety Coordinators with:

- the monitoring of the school Online Safety policy / documents
- the monitoring of the school filtering policy

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (at Foundation - parents / carers would sign on behalf of the pupils)
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- will be expected to report any concerns in relation to Online Safety to the Online Safety committee, who are also members the school council. Reporting can also take place directly to staff, via the worry box or via our website
- 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

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of technology than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Class Dojo and information about national / local Online Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy at Foundation stage.

Community Users

Community Users who access school ICT systems will be expected to use a specified log-in to access a restricted school network and systems.

5. 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 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 education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of computing / PHSE / other lessons and will be regularly revisited – this will cover both the use of devices and new technologies in school and outside school. Key Online Safety points for each topic are highlighted in the planning of the "Switched on Computing" scheme.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will 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 will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT equipment, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of ICT equipment, 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, pupils 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 Network Manager (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:

- Letters, newsletters, web site, Class Dojo
- Parents evenings / school performances / Parent drop in sessions
- Reference to the Childnet, ThinkUKnow and Common Sense Media websites, available through a link on the school website.

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community 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.

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:

- The Online Safety Coordinators (The Network Manager and computing lead) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others. This is then cascaded down to all staff.
- 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 school Online Safety policy and Acceptable Use Policies.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Coordinators will provide advice / guidance / training as required to individuals.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions

Technical – infrastructure / equipment, filtering and monitoring

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

- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance, including the "Keeping children safe in education" documentation 2019.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password. Pupils will have set generic log-ins, related to their year group. The Network Manager will keep an up to date record of users and their usernames. Staff will be required to change their passwords termly.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager will also be available to the Headteacher or other nominated senior leader.
- Users will be responsible for the security of their username and password.
- The school maintains and supports the managed filtering service provided by Netsweeper.
- The school provides different levels of access related to user's logins, to allow staff to access filtered content for appropriate educational content.
- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- The school filtering system is also applied to personal IT equipment, at the pupil's level of access.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the Network Manager, Computing Lead and the Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Computing Lead. If the request is agreed, this action will be recorded on the Netsweeper console and such actions shall be discussed by the Online Safety Committee
- The Network Manager monitors the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used to view user's activity. A back-up system is in operation within the site, but away from the servers. There is also an off-site backup, hosted by Scomis
- An appropriate system is in place for users to report any actual / potential online safety incident to the Online Safety Coordinators.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed procedure is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school (see School Personal Data Policy).
- An agreed procedure is in place that allows staff to install programmes on school workstations / portable devices after consultation with the Network Manager.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices (see School Personal Data Policy).
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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.
- 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 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, in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on newsletters, school documents, Class Dojo or the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 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.
- See Data protection policy for further details.

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.
- Lock their computer when leaving it unattended.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB 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 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			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	•						•	
Use of mobile phones in lessons				•				•
Use of mobile phones in social time	•							•
Taking photos on mobile phones or personal camera devices				•			•	
Use of personal hand held devices eg PDAs, PSPs	•						•	
Use of personal email addresses in school, or on school network		•						•
Use of school email for personal emails	•							•
Use of chat rooms / facilities				•				•
Use of instant messaging		•						•
Use of social networking sites			•					•
Use of blogs eg Class Dojo/School Jotter		•					•	

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 need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, Class Dojo 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 public chat / social networking programmes must not be used for these communications.

- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- 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

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's Online Safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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/academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

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

School staff should ensure that:

- No reference should be made in social media to students / 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.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee 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 certain internet usage as follows:

- 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

- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred and radicalisation
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Netsweeper and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming (non educational)
- On-line gambling
- Use of social networking sites
- Use of video broadcasting unless for educational purposes eg Youtube

Reporting of Online Safety incidents

Any incidents relating to Online Safety should be reported immediately to one of the following people:
Pupils to their class teacher / responsible adult they may be working with.
Other users should report any incidents to the Network Manager and the Computing Lead and complete an Online Safety incident form.
Online Safety concerns will be stored electronically in a secure folder on the network and reviewed by the Network Manager and Computing Lead. Appropriate actions will be taken in accordance with the Online Safety policy. Incidents relating directly to pupils will be recorded as a cause for concern via the “My Concern” online reporting system.

Responding to incidents of misuse

Illegal Incidents

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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

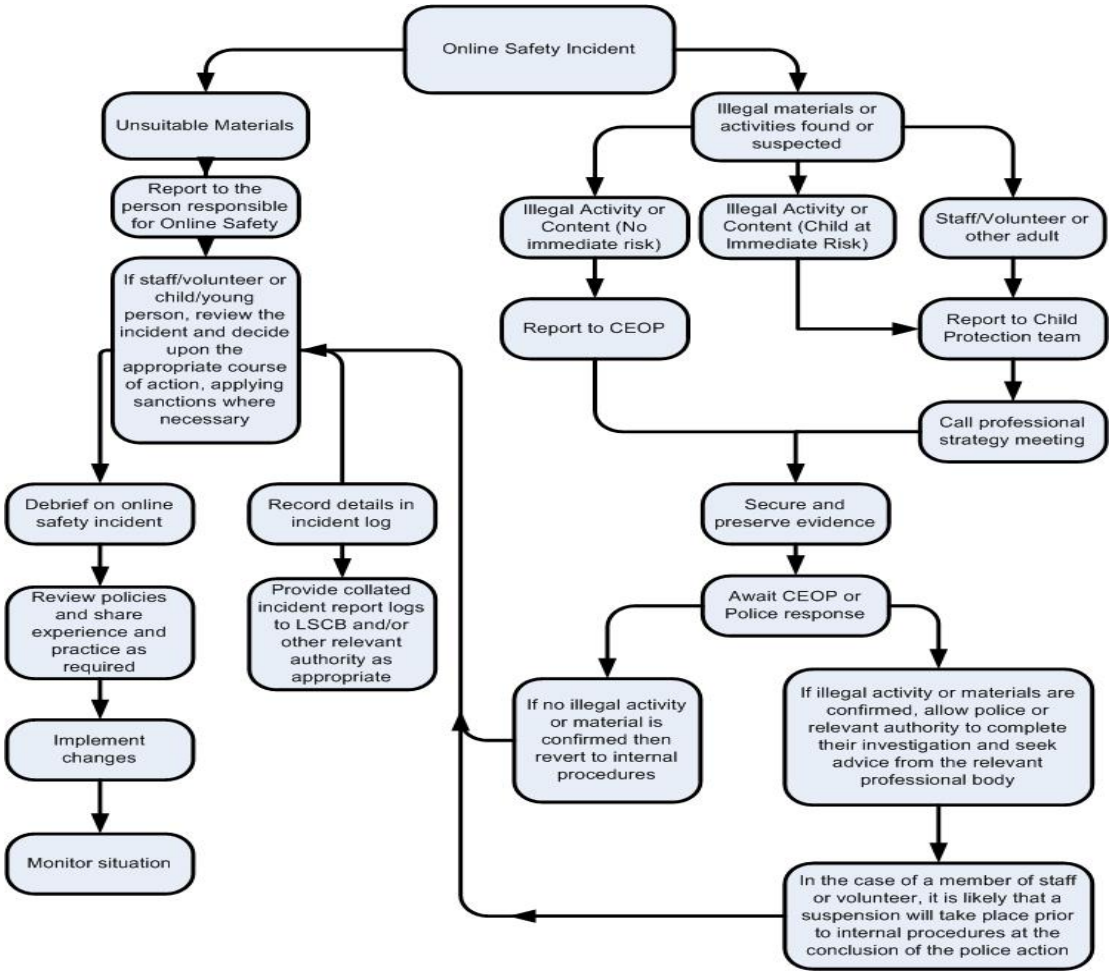
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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:	Refer to class teacher / tutor	Refer to ICT Managers (actions re filtering or security may be taken)	Refer to Headteacher	Refer to Police	Inform parents / carers	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	●	●	●	●	●	●
Unauthorised use of non-educational sites during lessons	●					●
Unauthorised use of mobile phone / digital camera / other handheld device	●					●
Unauthorised use of social networking / instant messaging / personal email	●	●	●		●	●
Unauthorised downloading or uploading of files	●	●	●		●	●
Allowing others to access school network by sharing username and passwords	●	●	●		●	●
Attempting to access or accessing the school network, using another pupil's account	●	●	●		●	●
Attempting to access or accessing the school network, using the account of a member of staff	●	●	●		●	●
Corrupting or destroying the data of other users	●	●	●		●	●
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	●	●	●	●	●	●
Continued infringements of the above, following previous warnings or sanctions	●	●	●	●	●	●
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	●	●	●	●	●	●
Using proxy sites or other means to subvert the school's filtering system	●	●	●		●	●
Accidentally accessing offensive or pornographic material and failing to report the incident	●	●	●	●	●	●
Deliberately accessing or trying to access offensive or pornographic material	●	●	●	●	●	●
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	●	●	●	●	●	●

Staff

Incidents:	Refer to line manager & ICT Managers (changes may be made to filtering\security)	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Warning	Disciplinary action (this may incude suspension)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	●	●	●	●	●	●
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / 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 instant 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 into disrepute or breach the integrity of the ethos of the school	●	●	●	●	●	●
Using proxy sites or other means to subvert the school'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	●	●	●	●	●	●

Checked by: P GLOVER

Date updated: 02.03.21