Glen Park Primary School

E-Safety Policy

February 2018

1. Introduction

The E-Safety policy considers all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

The development and expansion of the use of ICT and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-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. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

The Policies referred to within the E-Safety Policy are recommended by SWGfL as being an essential part of any E-Safety Policy and are based on good practice and experience of incidents at schools across the region. The overriding theme of the E-Safety Policy is that safe internet access is an entitlement for all learners.

Glen Park E-Safety Policy has been tailored to the needs of Glen Park, through discussion within the Computing Curriculum Team consisting of Teaching and Support Staff.

Due to the ever changing nature of Information and Communication Technologies, Glen Park Computing Team will review its E-Safety Policy annually and if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

2. Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 e-safety policy should help to ensure safe and appropriate use.

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 e-safety policy is used in conjunction with other school policies (eg anti-bullying, safeguarding).

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 e-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.

3. Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the Computing Curriculum team made up of:

- *Staff – Steve Gibson, Liggy Rossiter, Linda Croft*

4. Schedule for Development / Monitoring / Review

The implementation of this e-safety policy will be monitored by the:	Computing Curriculum team
Monitoring will take place at regular intervals:	Yearly
The Governing Body will receive a report on the implementation of the e-safety policy generated by the Monitoring Group (which will include anonymous details of e-safety incidents) at regular intervals:	Yearly – Spring Term
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

• Logs of reported incidents (logged on CPOMs Headteacher and Curriculum lead to be tagged)

• SWGfL monitoring logs of internet activity

5. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors) 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 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Glen Park Primary 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 e-safety behaviour that take place out of school.

6. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Senior Leadership Team (SLT) and Governors. Who will receive regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Child Protection to include E-safety Governor.

The role of the Child Protection Governor will include:

- regular monitoring of e-safety incident logs (saved on CPOMS)
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Head Teacher and Senior Leaders:

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Head Teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher / 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 e-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 Network manager.
- The Head Teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Officer (Head Teacher):

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

- Takes joint responsibility with the Computing Curriculum Team in ensuring 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 the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents, which is logged and held by the Network Manager.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / committee of Governors.

ICT Curriculum Team:

- Takes joint responsibility with the E-Safety Officer in ensuring 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
- regular monitoring of e-safety incident logs (saved on CPOMs)
- regular monitoring of filtering / change control logs
- Attends relevant meetings

Network Manager / Technical staff:

The Network Manager is 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 e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-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
- SWGfL is informed of issues relating to the filtering applied by the Grid
- That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer / Headteacher
- 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 e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They log any E-Safety Issues on CPOMs ensuring they tag the Computing Lead and Headteacher

- Digital communications with pupils (email / voice) should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils' understand and follow the school e-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 computing activity in lessons, extra-curricular and extended school activities
- They are aware of e-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

Child Protection Officer:

should be trained in e-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

Computing Curriculum Team

Members of the Computing Curriculum will assist the E-Safety Officer with:

- The production / review / monitoring of the school e-safety policy / documents.
- The production / review / monitoring of the school filtering policy (if the school chooses to have one) - SWGfL
- The monitoring of the E-safety incidents on CPOMs
- The monitoring of the SWGfL monitoring logs of internet activity

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. nb. at KS1 it would be expected that 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.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy

7. 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing lessons through the Switched On Computing scheme of work and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key E-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 materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in the ICT suite and Library
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Reference to the SWGfL Safe website
- Parents evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A regular annual update of E-safety will be available for all staff
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Officer/Coordinator /Network manager will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator/Network manager will provide advice / guidance / training as required to individuals as required

Training – Governors

Child Protection Governor should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority Governor Development Team/ National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- School Computing systems will be managed in ways that ensure that the school meets the E-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular monitoring of the safety and security of school Computing systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school Computing systems. Details of the access rights available to groups of users will be recorded by the Network Manager.
- All users (Year 2 and above) will be provided with a username and password by the Network manager who will keep an up to date record of users and their usernames. Class logons and passwords will be used for Foundation and Year 1 Pupils.

- The “administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL
- 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 Head teacher.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E-Safety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School Computing technical staff regularly monitor and record 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 by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager as directed by the E-safety ‘Actions and Sanctions’ and ‘Unsuitable/ Inappropriate Activities’ .
- 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 policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy 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.
- An agreed policy is in place allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

7.7 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of Computing across the curriculum.

- 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, eg using search engines, 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager and E-Safety Coordinator can, if agreed, 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.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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 and defined areas	Allowed for selected staff	Not allowed	Allowed, to be handed in to office	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 other personal cameras devices				✓					✓
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 on personal mobile devices		✓							✓
Use of social media on personal mobile devices		✓							✓
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. Staff and pupils should therefore use only the school email service and Google Education Email to communicate with others when in school, or on school systems (eg by remote access).
- 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, 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.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use when needed.
- Pupils should 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.

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:

User Actions

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

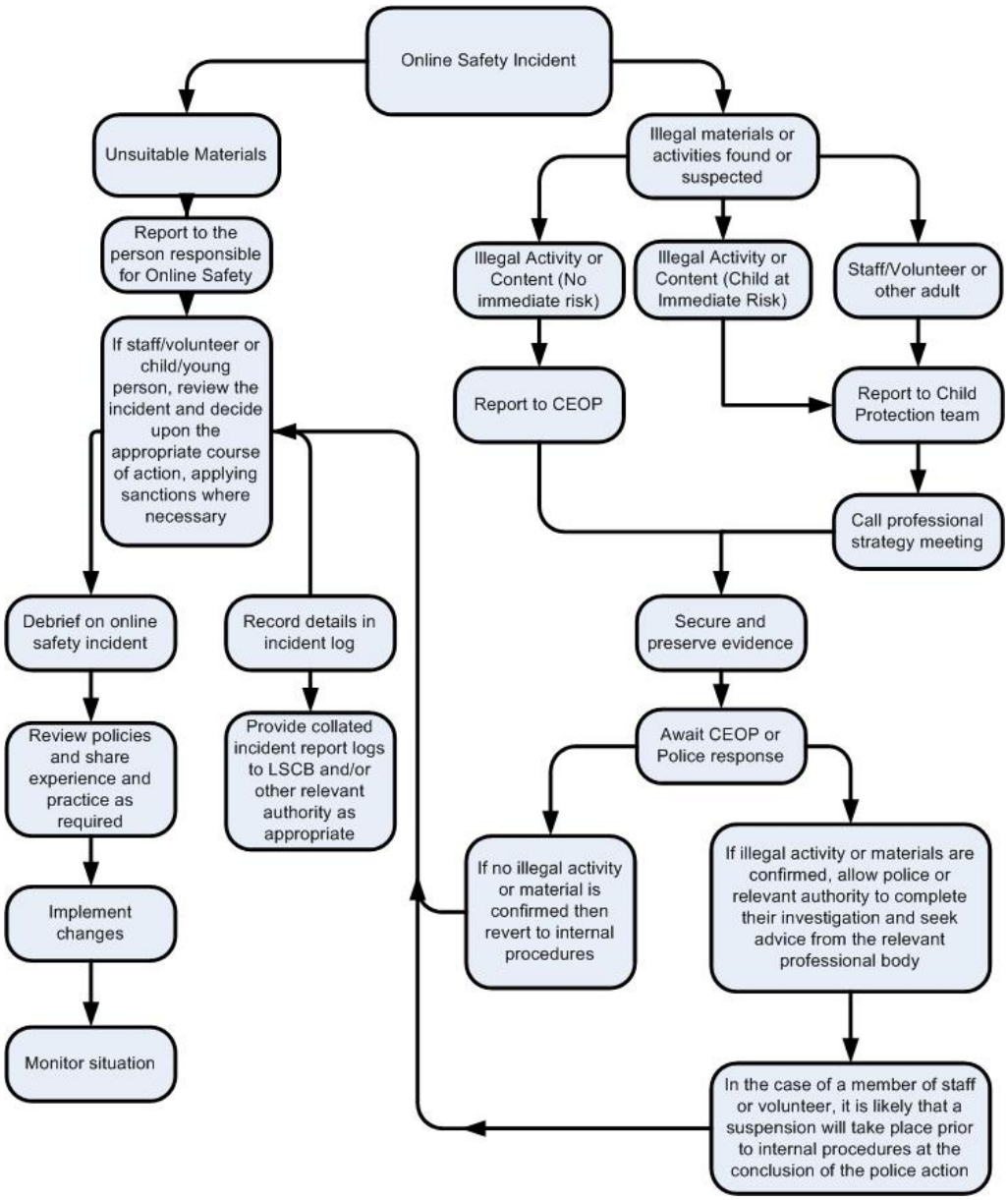
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this 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 – below 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.



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. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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 — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	✓				
Unauthorised use of non-educational sites during lessons	✓	✓		✓	✓		✓	
Unauthorised use of mobile phone / digital camera / other personal mobile device	✓	✓		✓	✓		✓	
Unauthorised use of social media / messaging apps / personal email	✓	✓		✓	✓		✓	
Unauthorised downloading or uploading of files	✓	✓		✓	✓		✓	
Allowing others to access school / academy network by sharing username and passwords	✓			✓			✓	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	✓			✓			✓	
Attempting to access or accessing the school / academy network, using the account of a member of staff	✓	✓		✓			✓	
Corrupting or destroying the data of other users	✓	✓					✓	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓		✓	
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 / 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	✓	✓		✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓		✓	✓	✓		✓

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		✓			✓	✓		
Unauthorised downloading or uploading of files		✓			✓	✓		
Allowing others inappropriate access to school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account inappropriately		✓	✓		✓	✓		
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 of a non-educational purpose eg SWGfl Proxy		✓	✓		✓	✓		
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		✓	✓	✓	✓			✓