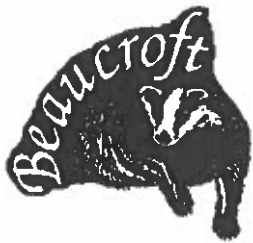



Beaucroft School

Online Safety (E-Safety) Policy

and

Acceptable Use Policies (AUP)



Issue Date: April 2023		April 2024
Date Adopted:		
Signed By: 		
Approval Committee: Governing Body		

Contents

Introduction / Rationale	3
Development / Monitoring / Review	4
How this policy has been developed	4
Schedule for Development / Monitoring / Review	4
How this policy will be monitored	5
Roles and Responsibilities	5
Governors.....	5
Headteacher & Senior Leaders.....	5
Online Safety Co-ordinator	6
ICT Support Staff.....	6
Teaching and Support Staff	7
Designated person for safeguarding	8
Students / Pupils.....	8
Parents / Carers	9
Community / Third Party Users	9
Policy Statements	9
Education and Training Policy Statement	9
Students & Pupils.....	9
Parents and Carers	9
Extended Schools	10
Staff	10
Governors	10
Technical Policy Statement.....	10
Curriculum Policy Statement.....	12
Use of Digital and Video Images.....	12
Data Protection Policy Statement	13
Social Media – Protecting Professional Identity	13
Communications Policy Statement	14
Unsuitable / Inappropriate Activities	15
Responding to Incidents of Misuse	17
Illegal / Criminal Activities.....	17
Policy Breach / Inappropriate (non-illegal) Activities	18
Students/Pupils	19
Staff	20

Introduction / Rationale

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

The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and students/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 always have an entitlement to safe internet access.

The requirement to ensure that children and young people can 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 students/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/student 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 (e.g., 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 students'/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 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.

Development / Monitoring / Review

How this policy has been developed

This policy has been developed in consultation with several interested parties, including:

- The School's Online Safety Co-ordinator
- The School's IT Systems Manager
- The Co-Headteachers and Senior Leaders
- Teachers and Support Staff
- Governors
- Parents and Carers

Schedule for Development / Monitoring / Review

This policy was adopted by the governing body on:	01/02/2019
The implementation of this policy will be monitored by:	The Online Safety Co-ordinator and the IT Systems Manager
Monitoring will take place at regular intervals:	Annually
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Annually
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:	A Year after the policy adoption/review date
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	Dorset Safeguarding Children's Board via the School's DSL and South West Grid for Learning

Online Safety Co-ordinator

The Online Safety Co-ordinator is:	Phil Childerhouse
------------------------------------	-------------------

- 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.
- Ensures the provision of training and advice for staff.
- Liaises with the Local Authority
- Liaises with school IT Systems Manager
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Meets as necessary with the Online Safety Governor to discuss current issues.
- Attends or provides reports to the Governor Teaching and Learning committee.
- Reports regularly to the Co-Headteachers

ICT Support Staff

IT Systems Manager	David Haysom
--------------------	--------------

- Ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensures 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.
- Ensures that users may only access the school's networks through a properly enforced password protection policy which passwords are regularly changed
- Informs SWGfL of issues relating to the filtering applied by the Grid.
- Ensures that the school's filtering policy is applied and updated on a regular basis, the responsibility for the implementation of which is shared with the Online Safety Co-ordinator
- Keeps up to date with Online Safety technical information to effectively carry out their Online Safety role and informs and updates others as relevant.
- Ensures that the use of the network/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator
- Uses monitoring software/systems which are implemented and updated regularly
- Ensures the safe storage of Staff, Student, Parent/Career and Visitor's signed Acceptable Use Policies (AUP) and that there is no access to the school's systems for any Staff, Student, Parent/Career or Visitor without a signed Acceptable Use Policy (AUP)

How this policy will be monitored

Beaucroft School will monitor this policy using a range of methods, including:

- Incident logs
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
 - Staff
 - Parents / Carers
 - Students / Pupils

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 ~~Teaching and Learning~~ Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

Reviews & Health & Safety

The role of the Online Safety Governor may include:

- Meetings with the Online Safety co-ordinator and IT Systems Manager
- Monitoring of Online Safety incident logs
- Monitoring of filtering/change control logs

Co-Headteachers & Senior Leaders

The Co-Headteachers are:	Joe Barnett and Diane Makariou
The Senior Leadership Team is made up of:	Sally Norman, Helen Harrison, Emma Wood, Rob Sallows

The Co-Headteachers are 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-ordinator

- The Co-Headteachers are responsible for ensuring that the Online Safety Co-ordinator 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 Co-Headteachers will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles. This will be through internal auditing and reporting as requested by the Co-Headteachers and responsible governor.
- The Co-Headteachers and other members 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.
- The Co-Headteachers will ensure that all staff have read, understood, and signed the requirements of the school's Acceptable Use Policy (AUP)

Teaching and Support Staff

- Ensure that they have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- Ensure that they have read, understood, and signed the current school Staff Acceptable Use Policy (AUP)
- Report any suspected misuse or problem to the Online Safety Co-ordinator
- Digital communications with students/pupils (email/voice/virtual learning environment only) should be on a professional level and only carried out using official school systems.
- Ensure that Online Safety issues are embedded in all aspects of the curriculum and other school activities
- Support students/pupils to the best of their ability in understanding and following the school Online Safety and Acceptable Use Policy (AUP)
- Monitor ICT activity in lessons, extra-curricular and extended school activities.
- 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 regarding these devices.
- in lessons where internet use is planned, ensure that all sites have been checked before the lesson and that students/pupils are guided to sites checked as suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches by reporting it to the school's IT Systems Manager and Online Safety Co-ordinator. Failure to do so could result in disciplinary action being taken.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) is:	Mandy Guy
--	-----------

The DSL 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

Students / Pupils

The following statements, as laid down within the model SWGfL policy, clearly must be considered and implemented in the context of the abilities and capabilities of each individual pupil/student at Beaucroft School. **As such it is assumed that various levels and degrees of support will be provided, as appropriate, to help everyone, understand and implement each statement;** indeed, there will pupils/students for whom these statements realistically will not apply due to the nature of their learning difficulties, but the basic principles nevertheless remain true and therefore remain appropriate to be stated within this policy.

- Are responsible for using the school ICT systems in accordance with the Student/Pupil Acceptable Use Policy (AUP), which they will be expected to sign before being given access to school systems.
- 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 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

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 the various communication channels in place.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy (AUP)
- Accessing the school website in accordance with the relevant school Acceptable Use Policy (AUP).

Community / Third Party Users

Community Users who access school ICT systems/website/VLE will be expected to sign the Staff, Volunteer & Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

Policy Statements

Education and Training Policy Statement

Students & Pupils

The education of students/pupils in Online Safety is 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, considering the context of individual capabilities:

- A planned Online Safety programme will be provided as part of PHSE and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key Online Safety messages will be reinforced within assemblies and tutorial/pastoral activities.
- Students/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.
- Students/pupils should be helped to understand the need for the student/pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Reference to rules for use of ICT systems/internet will be posted in all rooms and displayed on Login screens.
- Staff should act as good role models in their use of ICT, the internet, and mobile devices.

Parents and 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 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. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, website
- Parents' evenings

- Reference to the SWGfL Safe website (e.g., the SWGfL “Golden Rules” for parents)

Extended Schools

The school will aim to offer family learning courses in ICT, media literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Staff

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:

- All new staff will receive Online Safety awareness training as part of their induction programme. They will sign to acknowledge that they have read, understood, and agreed to the school's Acceptable Use Policy (AUP).
- Online Safety training will be reviewed at regular intervals, at least every year.
- The Online Safety Co-ordinator will receive regular updates through attendance at information/training sessions and by reviewing guidance documents released by relevant organisations and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings and INSET days.
- The Online Safety Co-ordinator will provide advice, guidance and training to individuals as required.

Governors

Governors should take part in Online Safety training/awareness sessions. This may be offered in several ways:

- Attendance at training provided by the Local Authority, National Governors Association or another relevant organisation.
- Participation in school training/information sessions for staff or parents.

Technical Policy Statement

Beaucroft will be responsible for ensuring that the school infrastructure/network is safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented; this responsibility is delegated to the Online Safety Co-ordinator and IT Systems Manager. It will also need to ensure that relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.

- School ICT systems will be managed as identified in the school technical security policy, Acceptable Use Policy (AUP) and any relevant Online Safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems, and cabling will be securely located and physical access restricted
- All users will have clearly defined rights to school ICT systems. Details of the access rights available to users will be recorded by the IT Systems Manager
- All users will be provided with a username and initial password by the IT Systems Manager or IT Systems Technician who will keep an up-to-date record of users and their usernames. It should be noted that cyber security advice has changed, and it is no longer recommended that Users be required to change their password every x days, this change is reflected in the technical security policy
- Class users may need to use class logins and passwords. Beaucroft School is aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in

this policy and the Acceptable Use Policy (AUP). Use by pupils/students should always be supervised and members of staff should never use a class login for their own network access.

- The school's ICT systems will be accessible at administrator level only by the IT Systems Manager and IT Systems Technician
- Users are legally responsible for the security of their username and password and 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 (Computer Misuse Act 1990)
- The school maintains and supports the managed filtering service provided by SWGfL.
- The IT Systems Manager will not switch off the filtering for any reason, or for any user. Individual staff can request the ability to switch off the SWGfL filtering for specific, educational purposes only using their own audited proxy access.
- Any filtering issues should be reported immediately to SWGfL by the IT Systems Manager
- Requests from staff for sites to be removed from the filter list will be considered by the IT Systems Manager and will be reported to the Online Safety Co-ordinator. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly
- The IT Systems Manager and Online Safety Co-ordinator regularly monitor and record the activity of users on school ICT systems and users are made aware of this in the Acceptable Use Policy (AUP). This monitoring includes, but is not limited to, the use of keylogging and device location (GPS) in the case of portable devices.
- Remote management tools are used by the IT Systems Manager, IT Systems Technician and the Online Safety Co-ordinator to control workstations and view user's activity.
- An appropriate system is in place for users to report any actual or potential Online Safety incident to the IT Systems Manager and the Online Safety Co-ordinator.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" or Bring Your Own Devices (BYOD) onto the school system.
- No software whatsoever is to be downloaded or installed on any school computer. The installation of new software applications must only be carried out by the IT Systems Manager or Technician
- Staff/students/pupils/community users and their family will not make personal use of any ICT equipment (e.g., laptops, portable devices, cameras, etc.) issued to them by the school.
- No memory sticks/USB keys/pen drives are allowed to be used for any reason. The IT Systems Manager or Technician may use these to install operating systems as appropriate.
- The school's infrastructure and individual workstations are protected by up-to-date anti-virus software. Staff will not use their personal services or hardware / computer for school related business.
- Professional data cannot be sent insecurely over the internet or taken off the school site.

Curriculum Policy Statement

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum. In particular:

- In lessons where internet use is planned, ensure that all sites have been checked before the lesson and that students/pupils are guided to sites checked as suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches by reporting it to the school's ICT technician and Online Safety Co-ordinator.
- Where students/pupils can freely search the internet, e.g. 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 (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Systems Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so will be logged, with clear reasons for the need.
- Where appropriate, students/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.
- Where appropriate, students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/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 students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
 - Staff can take digital/video images to support educational aims.
 - Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
 - Students/pupils must not take, use, share, publish or distribute images of others. This is an issue where the pupil is permitted to use or is issued with a school or personal portable device which will necessarily also have photo/video capturing capabilities. In these circumstances extra vigilance must be taken, by individually checking these devices, to ensure that this rule is adhered to.
 - Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
 - Students'/pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
-
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website.

Data Protection Policy Statement

This is not a replacement for the schools full Data Protection Policy it is a best practice statement.

Personal data will be recorded, processed, transferred, and made available in accordance with the General Data Protection Regulation 2018 which states that personal data must be processed in accordance with the following principles:

- Principle (a) – lawfulness, fairness, and transparency
- Principle (b) – purpose limitation
- Principle (c) – data minimisation
- Principle (d) – accuracy
- Principle (e) – storage limitation
- Principle (f) – integrity and confidentiality
- Accountability principle

Following several high-profile losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

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, ensuring that they are properly logged off at the end of any session in which they are using personal data.
- Transfer data using school systems and encryption.
- Personal Data should not be stored on any USB stick or any other removable media.

Social Media – Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees during their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

Communications Policy Statement

This is an area of rapidly developing technologies and uses.

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:

Communication Technologies	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Personal mobile phones may be brought to school	X				X			
Use of personal mobile phones in lessons				X				X
Use of personal mobile phones in social time	X						X	
Taking photos on personal mobile phones, tablets, or other camera devices			X Not of pupils					X
Use of personal hand-held devices e.g., PSP, DS in social time	X						X	
Use of personal email addresses in school, or on school network				X			X	
Use of school email for personal emails				X				X
Use of chat rooms/facilities				X				X
Use of instant messaging (For Work)	X							X
Use of social networking sites			X					X

Use of blogs				X			X	
--------------	--	--	--	---	--	--	---	--

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 students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users need to be aware that email communications can and may be monitored.
- Users must immediately report to the Online Safety Co-ordinator 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 students/pupils or parents/carers (email, VLE 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/websites, including but not limited to Facebook, Twitter, etc. must not be used for these communications.
- Students/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

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT 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, either because of the age of the users or the nature of those 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 (see next page):

User Actions

		Acceptable	Acceptable at certain times	Acceptable for certain 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					X
	promotion or conduct of illegal acts, e.g., under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred					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	
Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and/or the school					X	
Uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to						X

third parties, without the necessary licensing permissions					
Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)					X
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			X		
On-line gaming at school (educational)	X				
On-line gaming at school (non-educational)		X			
On-line gambling at school				X	
On-line shopping/commerce at school		X			
File sharing				X	
Use of social networking sites				X	
Uploading of videos e.g., YouTube				X	

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.

Illegal / Criminal Activities

If any apparent or actual misuse appears to involve illegal activity, e.g., activity that relates to child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity, or materials, the SWGfL flowchart should be consulted and actions followed in line with the chart; in particular, the sections on reporting the incident to the police and the preservation of evidence.

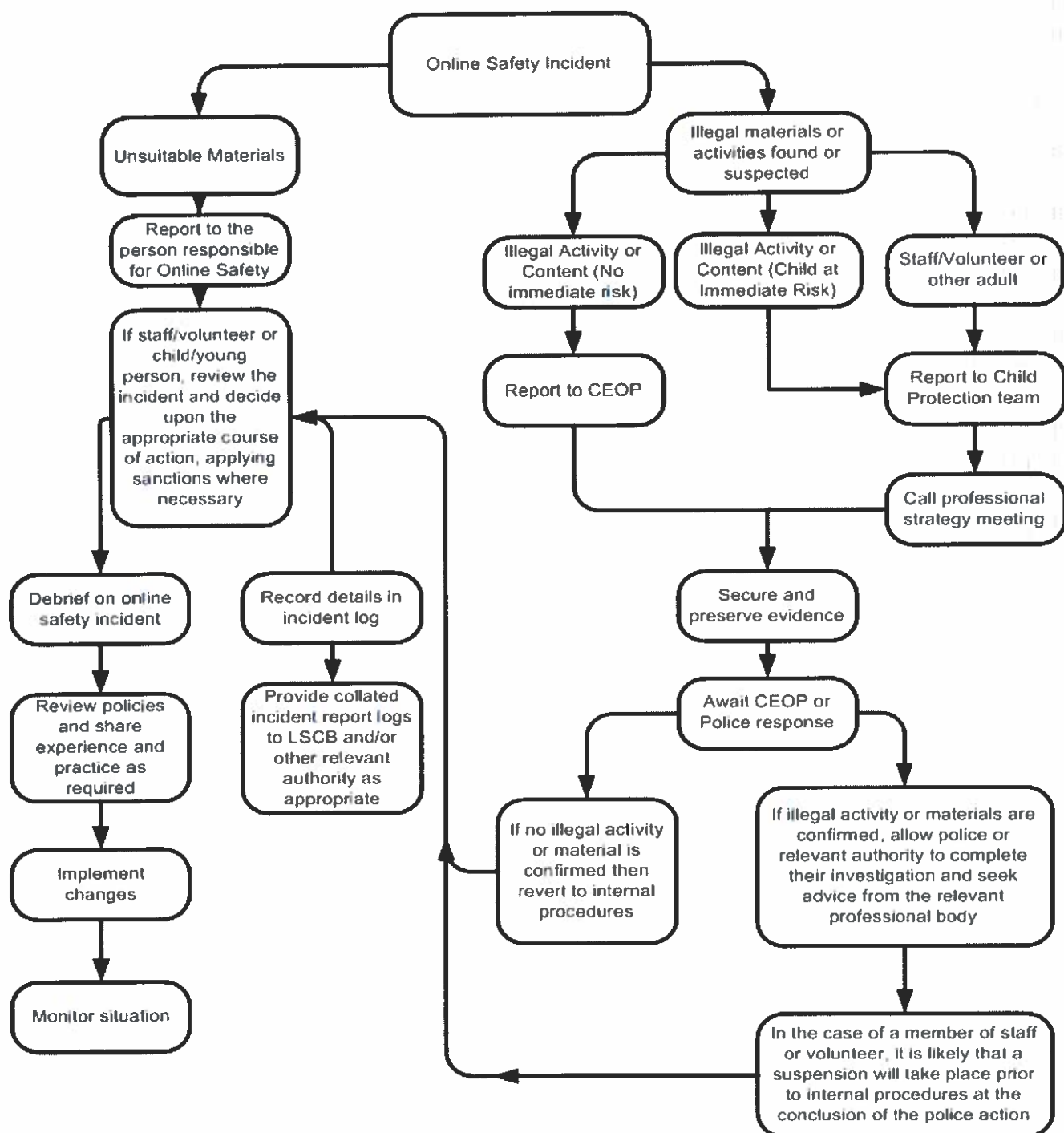


Figure 1 SWGfL Reporting Flow Chart

Policy Breach / Inappropriate (non-illegal) Activities

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:

Students/Pupils

Incidents: (A= Always, P=Potentially, N= Not Required)	Refer to class teacher/tutor	Refer to Head of Department	Refer to Headteacher	Refer to Police	Refer to technical support staff/Online Safety Co-	Inform parents/carers	Removal of network/internet access	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	A	A	A	A	A	A	A	A
Unauthorised use of non-educational sites during lessons	A	P	P	P	P	P	P	A
Unauthorised use of mobile phone/digital camera/another handheld device	A	P	P	P	P	P	P	A
Unauthorised use of social networking/instant messaging/personal email	A	P	P	P	P	P	P	A
Unauthorised downloading or uploading of files	A	P	P	P	P	P	P	A
Allowing others to access school network by sharing username and passwords	A	P	P	N	P	P	P	A
Attempting to access or accessing the school network, using another student's /pupil's account	A	P	P	P	P	P	P	A
Attempting to access or accessing the school network, using the account of a member of staff	A	A	P	P	P	A	P	A

Corrupting or destroying the data of other users	A	A	P	P	P	A	P	A
Continued infringements of the above, following previous warnings or sanctions	A	A	A	P	P	A	A	A
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	A	A	A	P	P	A	A	A
Using proxy sites or other means to subvert the school's filtering system	A	A	P	N	A	A	A	A
Accidentally accessing offensive or pornographic material and failing to report the incident	A	P	P	P	A	A	P	A
Deliberately accessing or trying to access offensive or pornographic material	A	A	A	P	A	A	A	A
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	A	P	P	N	P	P	P	A

Staff

Incidents: (A= Always, P=Potentially, N= Not Required)	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to technical support staff/Online	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)	A	A	A	A	A	A	A	A
Excessive or inappropriate personal use of the internet/social networking	A	P	N	N	A	A	P	P

sites/instant messaging/personal email								
Unauthorised downloading or uploading of files	A	P	N	N	A	A	P	P
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	A	A	P	P	A	A	P	P
Careless use of personal data e.g., holding or transferring data in an insecure manner	A	P	P	N	A	A	P	P
Deliberate actions to breach data protection or network security rules	A	A	P	P	A	A	P	P
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	A	A	P	P	A	A	P	P
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	A	A	P	P	A	A	P	P
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	A	A	P	P	A	A	P	P
Actions which could compromise the staff member's professional standing	A	A	P	P	A	A	P	P
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	A	A	P	P	P	A	P	P
Using proxy sites or other means to subvert the school's filtering system	A	A	P	P	A	A	P	P

Accidentally accessing offensive or pornographic material and failing to report the incident	A	A	P	P	A	A	P	P
Deliberately accessing or trying to access offensive or pornographic material	A	A	A	A	A	A	A	A
Breaching copyright or licensing regulations	A	P	P	P	A	A	P	P
Continued infringements of the above, following previous warnings or sanctions	A	A	A	P	A	A	P	P