ST COLUMBA’S CATHOLIC BOYS’ SCHOOL

GOVERNORS’ POLICY STATEMENT

eSafety Policy

Head Teacher: Mr N Fisher
School Lead: Mr B Woodcock
Chair of Governors: Mrs J Johnson

Originator Date	June 2017
Review Date (Three Years)	Summer 2020

INTRODUCTION

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 students 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 at St Columba's Catholic Boys' School are bound. Our school eSafety Policy should help to ensure safe and appropriate use. The development and implementation of e-safety strategies is everybody's responsibility should involve all the stakeholders in a child's education from the Head Teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote 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; and
- 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 eSafety policy is used in conjunction with other school policies (e.g. Behaviour for Learning, Anti-Bullying and Safeguarding 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' 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 eSafety 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.

Policy Development and Consultation

This eSafety policy has been developed by the eSafety Committee made up of:

- School eSafety Coordinator – Mr B Woodcock;
- Deputy Head Teacher/Safeguarding Lead – Mr B Woodcock ;
- ICT Subject leader – Mr L Williams;
- SENCO- Mrs K Kallend;
- Student Council Representatives;
- ICT Technical staff- Mr A Dunne; and
- Parents and Carers

Consultation with the whole school community has taken place through the following:

- Staff meetings;
- Student Council;
- INSET Day;
- Governors' meetings;
- Parents' evenings; and
- School website and newsletters.

Schedule for Development/ Monitoring /Review

The implementation of this eSafety policy will be monitored by the:

- SLT;
- eSafety Committee;
- Subject Leaders;
- Heads of Year;
- Curriculum and Pastoral Committee; and
- Governors

Governors will receive a report on the implementation of the eSafety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) annually.

Should serious eSafety incidents take place, the Police, Safeguarding (LADO) will be informed.

The school will monitor the impact of the policy using:

- Logs of reported incidents;
- Internal monitoring data for network activity; and
- Surveys / questionnaires of:
    - Students (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey, Have Your Say);
    - Parents / carers views; and
    - Staff views and staff audit.

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 Head Teachers, 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 e-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 for Learning and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors: are responsible for the approval of the eSafety Policy and for reviewing its effectiveness. This will be carried out by the Curriculum and Pastoral Committee receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body (Mr Keith Kelly) has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

- Regular meetings with the eSafety Co-ordinator / Officer;
- Regular monitoring of eSafety incident logs;
- Regular monitoring of filtering control logs; and
- Reporting to relevant Governors' meetings

Head Teacher and Senior Leaders:

- The Head Teacher is responsible for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Co-ordinator / Officer.
- The Head Teacher / Senior Leaders are responsible for ensuring that the eSafety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their eSafety 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 eSafety 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 eSafety Co-ordinator / Officer.
- 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 eSafety allegation being made against a member of staff. (Appendix1 : Flowchart for responding to online safety incidents)

eSafety Coordinator/ Officer: At St Columba's Catholic Boys' School the named member of staff with a day to day responsibility for eSafety is Mr B Woodcock who is also Safeguarding Lead for the school. The deputy lead for eSafety is Mr L Williams. The responsibilities of the eSafety coordinator in the school are as follows:

- Leads the eSafety committee;
- Takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies/ documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place;
- Provides training and advice for staff;
- Liaises with the Local Authority;
- Liaises with school ICT technical staff;
- Receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments, (See Appendix 2);
- Meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering control logs;
- Attends relevant Governors ' meetings; and
- Reports regularly to Senior Leadership Team.

Network Manager / Technical staff: The Network Managers (Mr A. Dunne/Mr M. Solomon) 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 eSafety technical requirements outlined in the LGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority eSafety 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;
- 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 (see appendix "Filtering Policy Template" for good practice document);
- That they keep up to date with eSafety technical information in order to effectively carry out their eSafety 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 eSafety Co-ordinator /Head Teacher/ Senior Leader/ Head of ICT/ ICT Co-ordinator/ Class teacher/ Head of Year for investigation and follow up action; and
- 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 eSafety matters and of the current school eSafety policy and practices;
- They have read, understood and signed the school Staff Acceptable Use Policy Agreement (AUP);
- They report any suspected misuse or problem to the eSafety Co-ordinator/ Officer/ Head Teacher/ Senior Leader/ Head of ICT/ ICT Co-ordinator/ Class teacher/ Head of Year (as in the section above) for investigation and action or sanction ;
- Digital communications with students (email / Virtual Learning Environment (VLE)/ voice) should be on a professional level and only carried out using official school systems;
- eSafety issues are embedded in all aspects of the curriculum and other school activities;
- Students understand and follow the school eSafety and Acceptable Use Policy;
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They are aware of eSafety 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; and
- In lessons where internet use is pre-planned students 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 eSafety 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; and
- Cyber-bullying.

All of the above are child protection issues and as such will be dealt with by trained safeguarding staff and not technicians. The new technologies in such cases are the vehicles for unacceptable safeguarding practices and not technical issues as such.

eSafety Committee: Members of the eSafety committee (or other relevant group) will assist the eSafety Coordinator with the production, review and monitoring of the school eSafety policy and documents.

At St Columba's representation on the eSafety committee is comprised of SLT, SENCO, Governing Body, students and technical support staff.

Students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems;
- 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; and
- should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety 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/ VLE and information about national/ local eSafety campaigns/ literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy; and
- Accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

POLICY STATEMENTS

Education – students: Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in eSafety is therefore an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience and know how to stay safe whilst using new technologies. eSafety education will be provided in the following ways:

- A planned eSafety programme should be provided as part of ICT other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and extended tutor periods;
- Students 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;
- Students should be helped to understand the need for the AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Students 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 all rooms and displayed on log-on screens; and
- 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 eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of 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, web site, VLE;
- Parents evenings and eSafety Workshops;
- Reference to the SWGfL Safe website (NB: the SWGfL “Golden Rules” for parents); and
- Providing links to the CEOP website

Education & Training – Staff: It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

- A planned programme of formal eSafety training will be made available to staff. An audit of the eSafety training needs of all staff will be carried out regularly. It is expected that some staff will be given the opportunity to identify eSafety as a training need within the performance management process. Staff have been audited (Sept.2012) and whole school staff e-safety training took place in October 2012;
- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies;
- The eSafety Coordinator will receive regular updates through attendance at LGfL/ Local Authority/ other information/ training sessions and by reviewing guidance documents released by BECTA / LGfL / the Local Authority and others;
- This eSafety policy and its updates will be presented to and discussed by staff in staff/ team meetings/ INSET days; and
- The eSafety Coordinator will provide advice/ guidance / training as required to individuals as required.

Training – Governors: Governors should take part in eSafety training/ awareness sessions, with particular importance for those who are members of any committee/ group involved in ICT/ eSafety/ 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 / LGfL or other relevant organisation; and
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

All the Schools servers and core switches are kept in a securely locked room.
All users have clearly defined access rights to the schools ICT system using network management software call RM CC4. This provides students with a locked down and secure user environment.
All users are provided with a username and password. The users are required to change their password every 60 days. Users are responsible for the security of their own 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 LGfL. In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by Head Teacher (or other nominated senior leader). Any filtering issues should be reported immediately to LGfL

Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and a nominated senior leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the eSafety Committee. School ICT 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
RM tutor is used by staff to control workstations and view student activity

Users can report any actual / potential e-safety incident to the Network Manager (or other relevant person) face-to-face, via the helpdesk, e-mail the Network Manager (or other relevant person), using the worry boxes around the school or by e-mailing reportit@st-columbas.bexley.sch.uk
Staff and student user accounts prohibit them from running executable files downloaded from the internet

The school infrastructure and individual workstations are protected by up to date virus software

Curriculum

KS3

All pupils have regular Starters & termly lessons dedicated to eSafety. They produce creative documents to illustrate learning & to help users stay safe online. Homework also develops and consolidates understanding of eSafety.

www.ictworkout.co.uk is a subscription that is currently being looked at to help engage pupils with eSafety topics.

KS4

The Cambridge Nationals has a written examination element, and theory around eSafety will be embedded to raise awareness.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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.

Where children are 'Looked After' the school will check consent on the corporate parent's behalf with the social worker. Where there are other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, this will require the need for extra care.

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 about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- 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;
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission. Children and young people may need to be made aware that taking and distributing inappropriate photographs may be a criminal offence;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;

- Students 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 are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix) Consent gained for photographs or videos may not extend to website or webcam use, so it is important to check, when introducing such technology, the status of existing consent for students or models; and
- Student's work can only be published with the permission of the student and parents or carers. Parents always retain the right to withdraw consent at any stage, but the school will require that they need to do so in writing.

Wide ranges of rapidly developing communications technology have 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 or disadvantages:

	Staff and other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobiles may be brought into school	✓					✓		
Mobiles used in lessons		✓					✓	
Mobiles used in breaks	✓							✓
Taking photos on mobile devices				✓				✓
Use of hand-held devices				✓				✓
Use of Personal email	✓						✓	
Use of school email for personal use	✓							✓
Use of Chat Rooms				✓				✓
Use of instant messaging	✓				✓			
Use of Social Networking sites			✓					✓
Use of blogs	✓						✓	

When using the following communication technologies, the school considers the following to be good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service 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 students or parents / carers (email, chat, 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 must not be used for these communications;

- Students will be provided with individual school email addresses for educational use. Students 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; and
- 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:

		Acceptable	Acceptable at certain times	Acceptable for nominated users only	Unacceptable	Unacceptable and illegal
Users shall not visit web 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 (e.g. under the child protection, obscenity, computer misuse & 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 religious or racial hatred				✓	
	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 it 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 LGfL 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 (e.g. 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 (educational)		✓			
On-line gaming (non-educational)				✓	
On-line gambling				✓	✓
On-line shopping / commerce				✓	
File sharing				✓	
Use of social networking sites				✓	
Use of video broadcasting e.g. YouTube		✓			

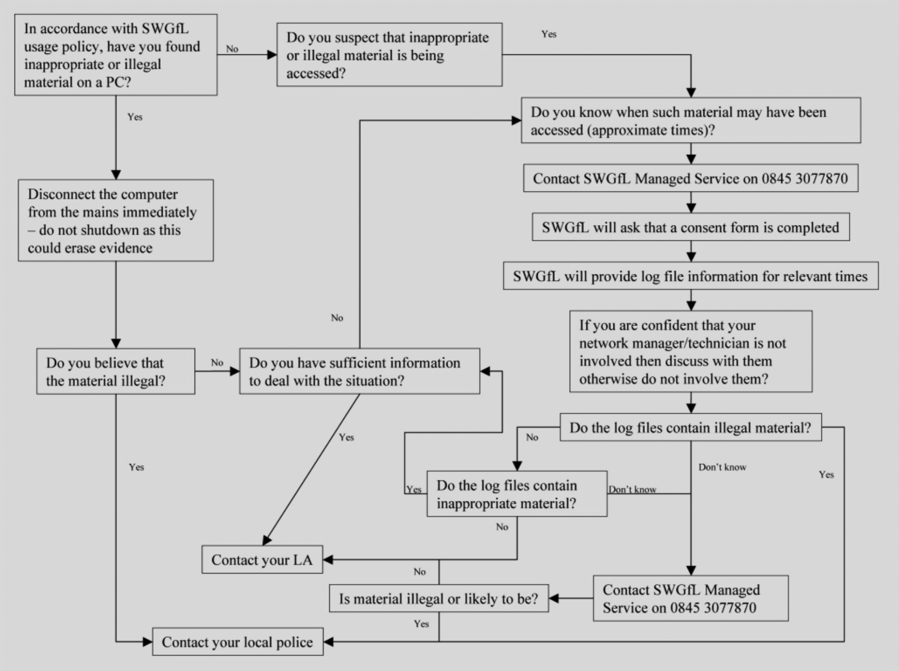
Responding to incidents of misuse

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 i.e.

- 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/ LGfL 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.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do the log files contain illegal material?
No
Don't know
Yes
Do the log files contain inappropriate material?
Yes
Don't know
No
Yes
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
No
Yes
Yes
Contact your LA
No
Is material illegal or likely to be?
Yes
Contact SWGfL Managed Service on 0845 3077870
Contact your local police

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 events, the LGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the LGfL 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	Refer to class teacher/ tutor	Refer to Head of Year	Refer to Head Teacher	Refer to Police	Refer to technical staff for action re: filtering	Inform parents/ carers	Removal of network/ internet rights	Warning	Further sanctions e.g. detentions, exclusion
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 student'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	Refer to Line manager	Refer to Head Teacher	Refer to Local Authority/ HR	Refer to Police	Refer to technical staff for action re: filtering	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).		✓	✓	✓	✓	✓	✓	✓
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 e.g. 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 carry out digital communications with students	✓	✓			✓	✓		
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		✓						✓

LIST OF APPENDICES

APPENDIX 1 – Flowchart for responding to online safety incidents

APPENDIX 2 – Staff & Volunteer Acceptable User Template

APPENDIX 3 – Student Acceptable User Template

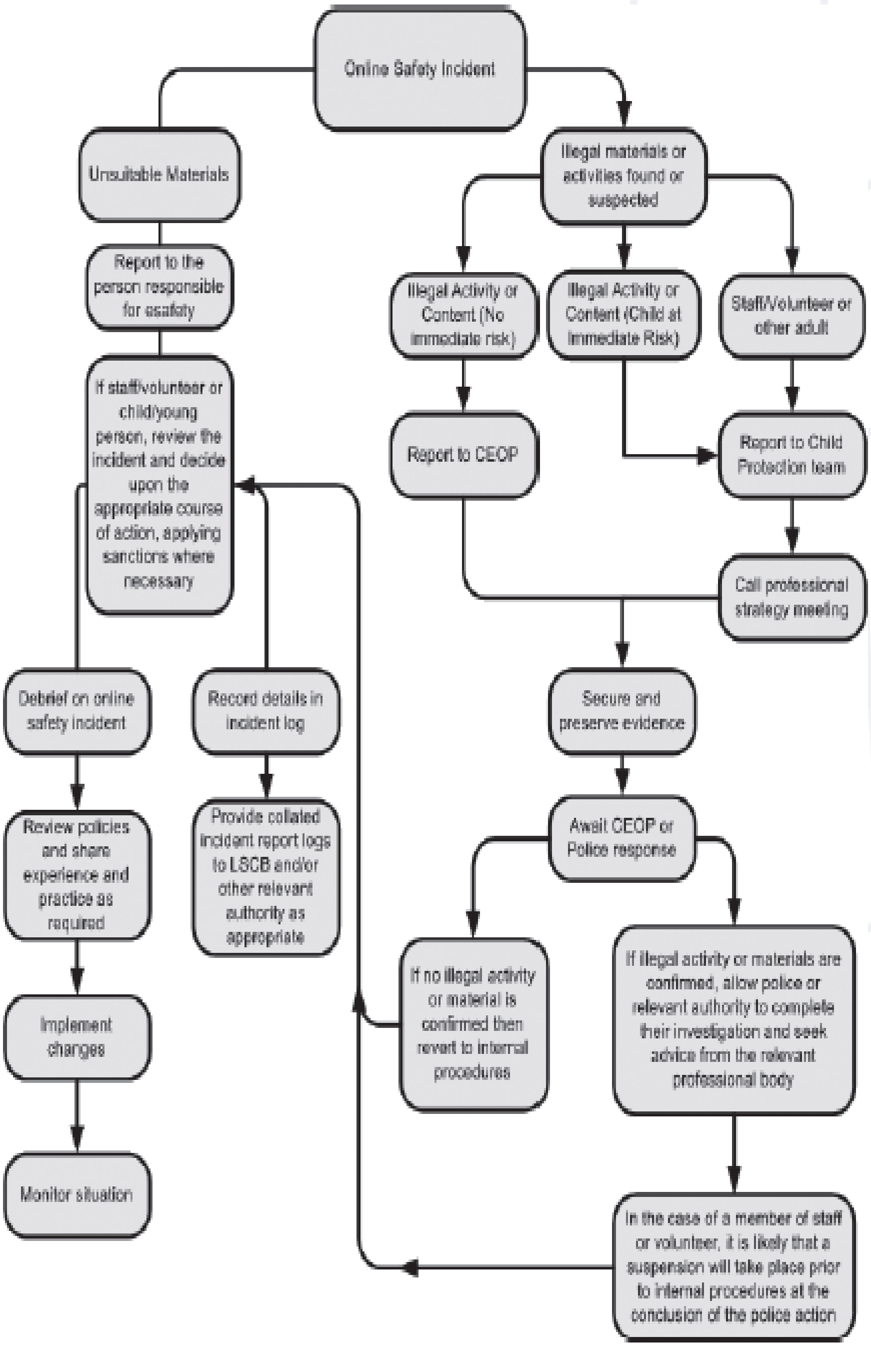
APPENDIX 4 – Charter for eSafety

APPENDIX 5 – Resources and Links

APPENDIX 6 – Glossary

APPENDIX 1

Flowchart for responding to online safety incidents


Online Safety Incident
Unsuitable Materials
Report to the person responsible for esafety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

APPENDIX 2

Staff and Volunteer Acceptable User Template

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk; and
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password; and
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these

images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured;

- I will only use chat and social networking sites in school in accordance with the school's policies;
- I will only communicate with students and parents and carers using official school systems. Any such communication will be professional in tone and manner. I will not use my personal email address or social networking identity for such communications;
- I will not use my personal mobile phone to contact parents or carers unless it is an emergency and there are no official school systems available; and
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems;
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes;
- I will ensure that my data is regularly backed up, in accordance with relevant school policies;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies;
- I will not disable or cause any damage to school equipment, or the equipment belonging to others;
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted;
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority; and
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work; and
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school; and

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: ……………………………………………….

Signed: ……………………………………………….

Date: ……………………………………………….

APPENDIX 3

Student Acceptable User Template

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk; and
- The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use the school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications;
- I will protect my username and password – I will not share it, nor will I try to use any other person's username and password;
- I will be aware of the dangers of talking to people I do no know, when I am communicating online;
- I will not disclose or share personal information about myself or others when online;
- If I arrange to meet people I do not personally otherwise know that I have communicated with online, I will do so in a public place and take an adult with me; and
- I will immediately report any unpleasant or inappropriate material, messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work; and
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions; and

- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones/ USB devices etc) in school if I have permission; I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will immediately report any damage or faults involving equipment or software, however this may have happened to the teacher supervising;
- I will not open any attachments to emails, unless I know and trust the person or organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings; and
- I understand it is strictly prohibited to use chat rooms and social networking sites on the school grounds.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos) unless sources are cited or otherwise instructed to do so; and
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information); and
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school);
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc; and
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: ……………………………………………….

Form: ……………………………………………….

Signed: ……………………………………………….

Date: ……………………………………………….

APPENDIX 4

Charter for eSafety

St Columba's Catholic Boys' School is working with staff, students and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential eSafety risks.

Our school community:

- Discusses monitors and reviews our eSafety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years;
- Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of eSafety across the whole school curriculum;
- Ensures that students are aware, through eSafety education, of the potential eSafety risks associated with the use of ICT and mobile technologies, that all eSafety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's eSafety policy.
- Provides opportunities for parents/carers to receive eSafety education and information, to enable them to support their children in developing good eSafety behaviour. The school will report back to parents/ carers regarding eSafety concerns. Parents/ carers in turn work with the school to uphold the e-safety policy.
- Seeks to learn from eSafety good practice elsewhere and utilises the support of the Local Authority, LGfL and relevant organisations when appropriate.

Chair of Governors: ____

Head Teacher: ____

Student Representative: ____

Date: ____

APPENDIX 5

Resources and Links

Links
The following links may help those who are developing or reviewing a school e-safety policy:
“SWGfL Safe” - http://www.swgfl.org.uk/safety/default.asp
Child Exploitation and Online Protection Centre (CEOP) http://www.ceop.gov.uk/
ThinkUKnow http://www.thinkuknow.co.uk/
CHILDNET http://www.childnet-int.org/
INSAFE http://www.saferinternet.org/ww/en/pub/insafe/index.htm
BYRON REVIEW (“Safer Children in a Digital World”) http://www.dcsf.gov.uk/byronreview/
Becta Website e-safety section - http://schools.becta.org.uk/index.php?section=is
Developing whole school policies to support effective practice -
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835
Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
“Safeguarding Children in a Digital World”
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344
London Grid for Learning http://cms.lgfl.net/web/lgfl/365
National Education Network NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html
CYBER-BULLYING
DfE - Cyberbullying guidance -
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007
Teachernet http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/
Teachernet “Safe to Learn – embedding anti-bullying work in schools”
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/
“How mobile phones help learning in secondary schools”:
http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482
Mobile phones and cameras:
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:
http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3
Links to other resource providers:
BBC Chatguides: http://www.bbc.co.uk/chatguide/index.shtml
Kidsmart: http://www.kidsmart.org.uk/default.aspx
Know It All - http://www.childnet-int.org/kia/
Cybersmart - http://www.cybersmartcurriculum.org/home/
NCH - http://www.stoptextbully.com/
Chatdanger - http://www.chatdanger.com/
Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm
Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx
London Grid for Learning: http://cms.lgfl.net/web/lgfl/safety/resources

APPENDIX 6

GLOSSARY

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Becta
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol