Burscough Priory Science College

e-SAFETY POLICY

(and new technologies)

BACKGROUND/RATIONALE

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and 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 in schools are bound. Burscough Priory's eSafety policy helps to ensure safe and appropriate use of these technologies. The development and implementation of our strategy involves all the stakeholders in your 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 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 our eSafety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build 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. As a school, we 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.

DEVELOPMENT, MONITORING, REVIEW OF THIS POLICY

This eSafety policy has been developed by Burscough Priory Science College by the:

- Headteacher/Senior Leaders
- School eSafety Champion
- eSafety Ambassadors
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

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

- Staff meetings
- School Council
- INSET Day
- Governors meeting/committee meeting
- School website/newsletters

SCHEDULE FOR DEVELOPMENT, MONITORING, REVIEW

This eSafety policy was approved by the *Governing Body on:*	3.02.2011 for initial approval.
The implementation of this eSafety policy will be monitored by the:	*All staff and Governors of the school.*
Monitoring will take place at regular intervals:	*Termly*
The *Governing Body* will receive a report on the implementation of the eSafety policy generated by the monitoring group (which will include anonymous details of eSafety incidents) at regular intervals:	*Termly*
The eSafety 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 eSafety or incidents that have taken place. The next anticipated review date will be:	*October 2014 with Gov committee Spring term 2015*
Should serious eSafety incidents take place, the following external persons/ agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents using school 'worry forms'
- Internal monitoring data for network activity
- Surveys/questionnaires of students, parents/carers and staff

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 eSafety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate eSafety behaviour that take place out of school.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school:

GOVERNORS:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors/ Governors Sub Committee* receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

- regular meetings with the designated eSafety Co-ordinator
- regular monitoring of eSafety incident logs
- reporting to relevant Governors committee/meeting

HEADTEACHER AND SENIOR LEADERS:

- The Headteacher 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.
- The Headteacher/Senior Leaders are responsible for ensuring that the eSafety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. All staff will be provided with a copy of the incident flow chart in order to deal with each incident effectively.
- The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the eSafety Co-ordinator.
- The Headteacher and another member of the Senior Leadership Team/Senior Management 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. (see flow chart on dealing with eSafety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures)

CHILD PROTECTION AND ESAFETY CHAMPION: K WALTON

The Child Protection Officer is trained in eSafety issues and also aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

The Designated eSafety Champion takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies/documents as well as:

- 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 holds a log of incidents to inform future eSafety developments. The log will be kept by the e safety champion on the staff SLT secured shared area. The log can be viewed if appropriate on request.
- liaises regularly with the eSafety Governor to discuss current issues, review incident logs and filtering/change control logs (TBA in Autumn Term each Year.)
- reports regularly to Senior Leadership Team

ESAFETY AMBASSADORS : C BLUNDELL & K COLLINS

The eSafety Ambassadors role is to support the eSafety Champion by

- ensuring that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Providing specific training and advice for staff
- liaising with school ICT technical staff
- reporting regularly to the eSafety Champion
- running a monthly Stay Safe Committee

NETWORK MANAGER/TECHNICAL STAFF:

The ICT Technician/ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the eSafety technical requirements as advised by Becta and the Acceptable Use Policy.
- 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.
- that he/she keeps 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 and Learning Platform is regularly monitored (daily) in order that any misuse/attempted misuse can be reported to the eSafety Co-ordinator.
- that monitoring software/systems are implemented and updated as agreed in school policies.

TEACHING AND SUPPORT STAFF

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 Policies/Agreements (including Mobile Phones & Cameras Agreement and Social Networking Agreement).
- they report any suspected misuse or problem to the eSafety Co-ordinator/ Headteacher
- digital communications with students/pupils (email/Learning Platform) should be on a professional level
- 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
- 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

STAY SAFE COMMITTEE

Members of the Stay Safe Committee will assist the eSafety Champion with the production/review/monitoring of the school eSafety policy/documents. The Stay Safe Committee will also consist of students. The main goal will be to help review and monitor esafety in and around school, including elements outside of school.

STUDENTS/PUPILS:

- are responsible for using the school ICT systems in accordance with the Student/Pupil 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.
- 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, and the school website/Learning Platform.*

Parents and carers will be responsible for endorsing (by signature) the Student Acceptable Use Policy.

COMMUNITY USERS

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

ESAFETY CURRICULUM FOR 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. eSafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.

- eSafety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- eSafety skills should be embedded through both discrete ICT and cross-curricular application.
- A planned eSafety programme should be also provided as part of form times and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites visited.
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Rules for use of ICT systems/internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

ESAFETY EDUCTION FOR 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 the children's online 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, learning platform
- Parents' evenings

ESAFETY EDUCAITON FOR EXTEDNED SCHOOLS

The school will offer learning courses in ICT, media literacy and eSafety so that parents and children can together gain a better understanding of these issues. Messages to the public around esafety should also be targeted towards grandparents and other relatives as well as parents. 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.

ESAFETY EDUCATION & TRAINING FOR 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:

- An audit of the eSafety training needs of all staff will be carried out regularly and training needs will be incorporated into staff meetings/INSET planning.
- 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 Champion (and Ambassadors) will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/Lancashire and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days/emails.
- The eSafety Champion along with the Ambassadors will provide advice/guidance/training as required to individuals as required.

ESAFETY TRAINING FOR 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 or other relevant organisation.
- Participation in school training/information sessions for staff or parents/email updates.

ESAFETY INFRASTRUCTURE

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

- School ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined by Becta and the Acceptable Usage Policy.
- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smart board etc. must be kept current.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will be provided with a username and password to access the school network by the school ICT technician who will keep an up to date record of users and their usernames.
- All users of the school learning platform will be provided with a username and password for secure access in school and beyond.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place.
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- Users will be made 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.
- The school maintains and supports the managed filtering service provided by **EXA Networks**.
- 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 a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately the Network Manager.
- 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.
- An appropriate system is in place through the use of the school's "**Stay Safe**" form (from 1st October 14) for users to report any actual/potential eSafety incident to the designated eSafety Champion.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed system is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreement is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- Staff should not install programmes on school workstations/portable devices without getting consent from the Headteacher/Network manager.
- Staff sign the AUP where the agreement is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices.

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 about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that 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.
- 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.
- The office will have a log of the names of any pupil that should not have their picture used. Staff will need to refer to this before placing any photographs on the website.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

This is part of the Teachers' standards to take professional responsibility for data. The protocol will be reviewed as part of the e safety briefing at the start of each year.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

With CC4 anywhere there should be no need for staff to use USB or any other portable media. Therefore, we discourage the use of portable media. If portable media is used than the following must followed:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows a quick overview of what is allowed and not allowed -

	Staff and Other Adults	Students	
Communication Technologies (Outside of those available on the Learning Platform)	Allowed	Allowed at Certain Times	Not Allowed
Mobile phones may be brought into school.	✓	✓	
Use mobile phones in lesson (Please refer to mobile phone policy)	✓ With Heads Permission	✓Only in specified lessons with teacher consent.	
Use of mobile phones in social time	✓		✓
Taking photos on mobile phones or other camera devices	✓If on school registered phone of children with parental consent for display purposes.		✓
Use of handheld devices eg.g netbooks, PDAs, PSPs, Ipad, IPod	✓	✓In lessons with teacher consent.	
Use of personal email addresses in school, or on school network	✓ With Heads Permission		✓
Use of school email for personal emails	✓ With Heads Permission		✓
Use of chatroom/instant messaging facilities			✓
Use of social networking sites	✓		✓
Use of Twitter	✓		

When using communication technologies the school considers the following as good practice:

- Where available the official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content.
- 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Benefits of Department Use

- Promotes communication with parents/guardians and students.
- Instant notification of changes to extra-curricular timetable to students and parents/guardians.
- Sharing of links to internet based resources (clips, articles, revision websites etc)
- Celebrate student achievement and promote department activities.

Email Policy:

- All staff have access to the school's e-mail system.
- All digital communications should be professional in tone and content.
- Only official email addresses should be used to contact staff/pupils.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts so any incidents of SPAM should be reported to the network manager, Rob Frain, who can then contact the Westfield Centre.
- All staff and pupils should be aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All staff and pupils should be aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All staff and pupils are aware that all email communications may be monitored at any time in accordance with our **Acceptable Use Policies**.
- All staff and pupils must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

BPSC includes a standard disclaimer at the bottom of all our outgoing emails that states -
"This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Burscough Priory Science College. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000."

Social Networking Policy

- These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools.
- Any form of bullying or harassment is strictly forbidden and in the case of an incident involving a member of staff or a pupil, even if outside of school, staff must follow the **BPSC esafety Flow chart.**
- Pupils will be advised throughout the ICT curriculum never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to have images of themselves or peers in school uniform on Social Networking sites.
- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details on any social networking sites, blogs or personal websites.
- Staff must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Personal details must not be shared with pupils and privacy settings be set at maximum.
- Staff must not accept pupils as 'friends' on any Social Network site.
- Staff must not add ex-pupils as 'friends' on any Social Networking sites until the ex-pupil reaches the age of eighteen and even then, staff should use discretion on the decision.
- Staff should always conduct themselves in a professional manner whilst using a social networking site and avoid behavior which might be misinterpreted by others.
- Staff should not have any inappropriate images on a social networking site.
- Staff must not have their place of work listed on a social networking site.
- Staff should not become members on any inappropriate groups on a social networking site.An inappropriate group site includes those sites which allow personal details to be shared openly to the community.
- Pupils are advised in assemblies, via form teachers and in lessons of the dangers of social networking sites.

Instant Messaging Policy

- Instant Messaging, e.g. MSN, Skype, Yahoo Messenger, is blocked in school.
- Any form of bullying or harassment is strictly forbidden and in the case of an incident involving a member of staff or a pupil, even if outside of school, staff must follow the **BPSC esafety Flow chart.**

Video Conferencing Policy

- Pupils must have signed a permissions letter before taking part in kind of video conferencing.
- Approval by the Headteacher must be obtained in advance of the video conference taking place
- All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.

Twitter/Instagram Policy

- Not to follow any students (past or present) or Parents/Guardians.
- Direct Messages (D.M'S) not to be used to contact or reply to any students or Parents/Guardians.
- No overlap between personal and department twitter accounts. Do not retweet content from either account.
- Due care and consideration must be taken before sending any tweet. Content should only be tweeted if its appropriate for a classroom environment.
- Any department accounts that have been created but are not being maintained should be deactivated.
- Department Twitter should essentially be treated as an interactive notice board.
- In the interest of safeguarding all accounts will be overseen by KW.
- A named member of the department should be point of contact for of the account.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as seen in the chart on the next page:

User Actions

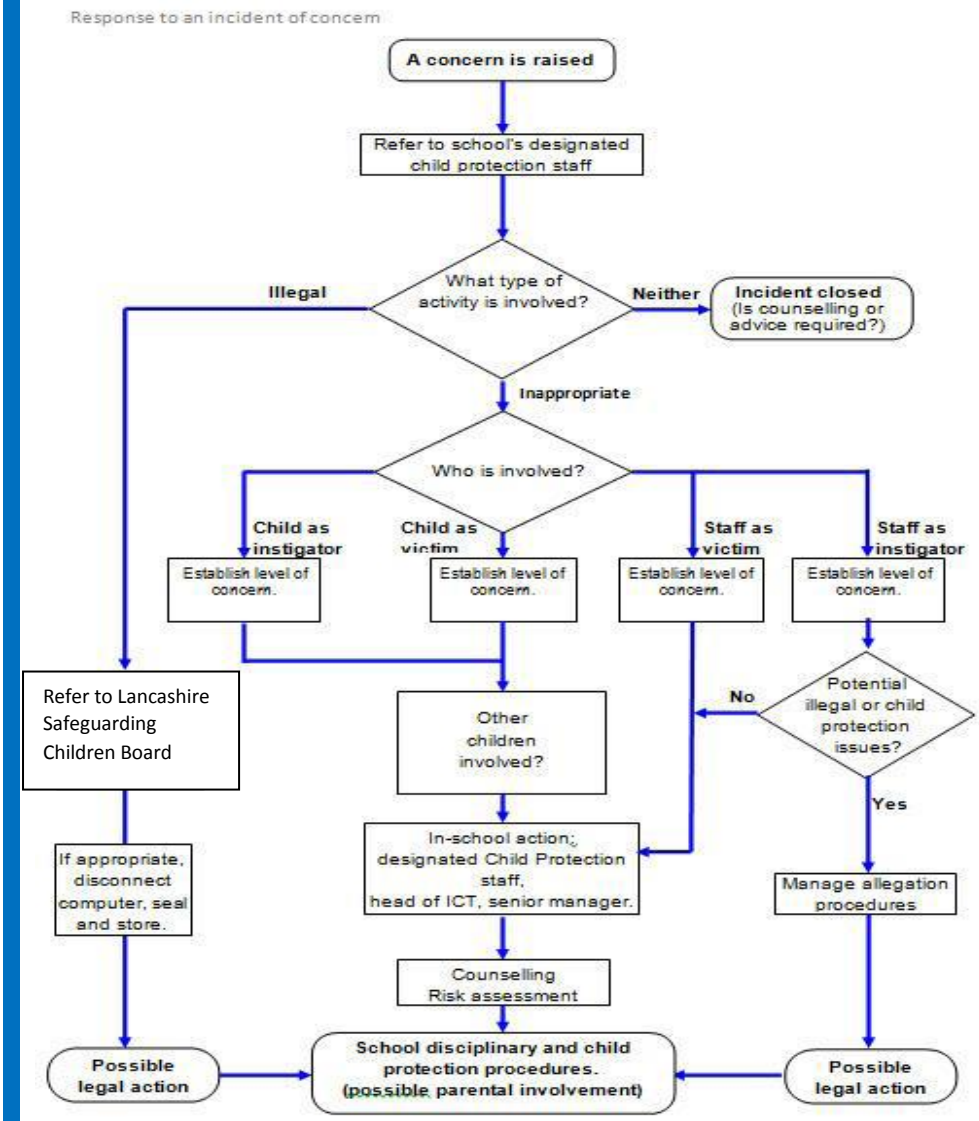
		Acceptable	Acceptable at Certain Times	Acceptable for Nominated Users	Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images				✓	✓
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	Adult material that potentially breaches the Obscene Act in the UK				✓	✓
	Criminally racist material				✓	✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Promotion of any kind of racial or religious hatred				✓	
	Threatening behaviour, including the promotion of physical violence/mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by WBC and/or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)					✓	
Creating/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					✓	
Online gaming (educational)			✓			
Online gaming (non educational)					✓	
Online gambling					✓	
Online shopping/commerce					✓	
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
- other criminal conduct, activity or materials
-

The BPSC eSafety 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. (A larger copy of this flow chart is attached to the end of the policy.)



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

Incidents:	Refer to Class Teacher	Refer to HOD or Head Of Year	Refer to Headteacher	Refer to Police	Refer to Network Manager	Inform Parents/Carers	Removal of network/Internet Access	Warning	Further sanctions detention/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	✓	✓ 3rd	✓		✓			✓ 1st	✓ 2nd
Unauthorised use of mobile phone/digital camera/other handheld device			✓			✓		✓	
Unauthorised use of social networking/instant messaging/personal email	✓	✓ 3rd						✓ 1st	✓ 2nd
Unauthorised downloading or uploading of files	✓	✓ 3rd			✓			✓ 1st	✓ 2nd
Allowing others to access school network by sharing username and password			✓		✓	✓	✓	✓ 1st	✓ 2nd
Attempting to access or accessing the school network, using another student's/pupil's account			✓		✓	✓	✓		✓ 1st

Students Actions/Sanctions

Incidents:	Refer to Class Teacher	Refer to HOD or Head Of Year	Refer to Headteacher	Refer to Police	Refer to Network Manager	Inform Parents/Carers	Removal of network/Internet Access	Warning	Further sanctions detention/exclusion
Attempting to access or accessing the school network, using the account of a member of staff			✓		✓	✓	✓		✓ 1st
Corrupting or destroying the data of other users			✓		✓	✓	✓		✓ 1st
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓ further			✓	✓	✓ Possible		✓ 1st
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					✓		✓ Possible		✓ 1st
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓			✓	
Deliberately accessing or trying to access offensive or pornographic material			✓	✓	✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓		✓			✓	

Staff

Actions/Sanctions

Incidents:	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Network Manager	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	✓	✓	✓		✓	✓	Possible	Possible
Unauthorised downloading or uploading of files		✓	✓		✓	✓	Possible	Possible
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		✓	✓		✓	✓	Possible	Possible
Careless use of personal data eg holding or transferring data in an insecure manner		✓				✓		
Deliberate actions to breach data protection or network security rules		✓	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓		✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓		✓	✓	Possible	Possible
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		✓	✓		✓	✓	Possible	Possible
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		✓	✓			✓	Possible	Possible

Staff Actions/Sanctions

Incidents:	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Network Manager	Warning	Suspension	Disciplinary action
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	Possible	Possible
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	✓	✓	✓		✓	✓	✓	✓

ACKNOWLEDGEMENTS

Burscough Priory would like to acknowledge and thank a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School eSafety Policy Template:

- SWGfL eSafety Group
- LCC
- Christ Church C.E. of Warrington
- DCSF
- Becta
- National Education Network (NEN)
- Byron Review – Children and New Technology – "Safer Children in a Digital World"

LEGISLATION

Schools should be aware of the legislative framework under which this eSafety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

COMPUTER MISUSE ACT 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

DATA PROTECTION ACT 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

COMMUNICATIONS ACT 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

MALICIOUS COMMUNICATIONS ACT 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

REGULATION OF INVESTIGATORY POWERS ACT 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

TRADE MARKS ACT 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

COPYRIGHT, DESIGNS AND PATENTS ACT 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

TELECOMMUNICATIONS ACT 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

CRIMINAL JUSTICE & PUBLIC ORDER ACT 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

RACIAL AND RELIGIOUS HATRED ACT 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

PROTECTION FROM HARASSMENT ACT 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions

PROTECTION OF CHILDREN ACT 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

SEXUAL OFFENCES ACT 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

PUBLIC ORDER ACT 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

OBSCENE PUBLICATIONS ACT 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

HUMAN RIGHTS ACT 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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.

LINKS TO OTHER ORGANISATIONS OR DOCUMENTS

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 eSafety 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 eSafety 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
NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp
NATIONAL EDUCATION NETWORK
NEN eSafety Audit Tool: **http://www.nen.gov.uk/hot_topic/13/nen-eSafety-audit-tool.html**
CYBER-BULLYING
DCSF - 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/**
SOCIAL NETWORKING
Home Office Task Force - Social Networking Guidance -
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce
Digizen – "Young People and Social Networking Services":
http://www.digizen.org.uk/socialnetworking/
Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/
MOBILE TECHNOLOGIES
"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

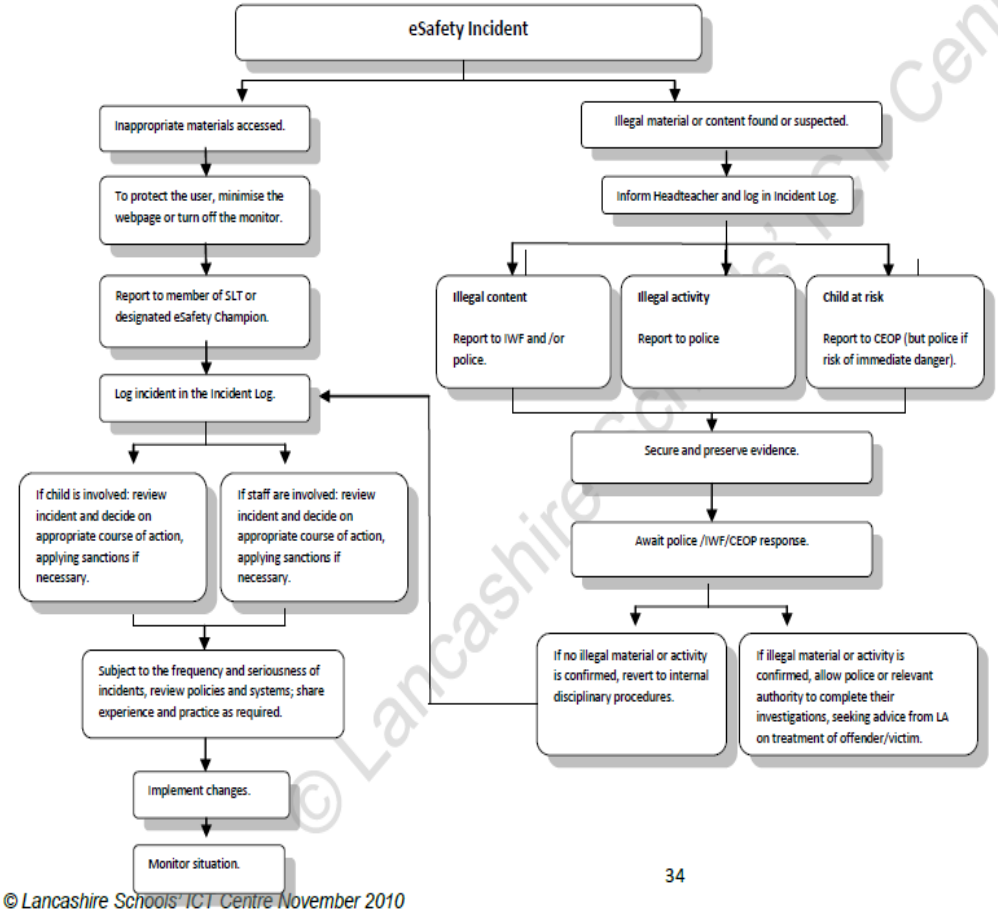
DATA PROTECTION AND INFORMATION HANDLING
Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx
BECTA - Data Protection:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03
PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

RESOURCES
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**

GLOSSARY OF TERMS

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 A learning platform brings together hardware, software and supporting services
Platform to support teaching, learning, management and administration.
LSCB Local Safeguarding Children Board
MIS Management Information System
MLE Managed Learning Environment
NEN National Education Network
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
NWGfL North West Grid for Learning – the Regional Broadband Consortium of NW Local Authorities
TUK Think U Know – educational eSafety programmes for schools, young people and parents.
VLE Virtual Learning Environment
WAP Wireless Application Protocol

APPENDIX 11 – Responding to eSafety Incident/ Escalation Procedures



Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp

LCC Schools' eSafety Lead

Lancashire Schools' ICT Centre
(01257) 516360
info@ict.lancsngfl.ac.uk

Securing and Preserving Evidence – Guidance Notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system).
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
- Make a note of the date / time of the incident along with relevant summary details.
- Contact your School's Neighbourhood Policing Team for further advice.

34

Appendix 12 – BPSC Staff e Safety Incident Form

Date	
Pupil(s) involved	
Details of Incident	
1st Member of Staff Reported To and Action/Impact	
2nd Member of Staff Reported To and Action/Impact	
3rd Member of Staff Reported To and Action/Impact	
4th Member of Staff Reported To and Action/Impact	
Has the incident been actioned and resolved? If yes, file form in secure place.	E safety champion or ambassador to sign below.

BPSC'S E-SAFETY POLICY PROCEDURE:

Disclosure relating to an E Safety Incident

If a Child approaches you with an E Safety Incident:

1. Do not promise to keep it to yourself. If it is related to cyberbullying or online abuse, advise the student not to respond to any messages and to secure any evidence.

2. A Staff e Safety Incident log to be filled in by the Member of Staff who the student approached and also any other staff involved in the incident.

3. If the incident also raises child safeguarding concerns. A further child protection form will have to be filled in.

4. Pass the incident form (or forms) on to the most appropriate person. This might include a number of staff, but choose the most appropriate starting point.*
    a. Class Teacher
    b. Form teacher
    c. HOY
    d. Network Manager
    e. SLT/Police
    f. The school's e-safety Champion (KW) or Ambassador (CB).
    g. Child Protection Officer (KW)

5. Actions and impact will be recorded on the form by all those involved and finally passed on to the e safety Champion (KW) or e safety Ambassador (CB) to make sure that the incident has been actioned, resolved and filed in a secure place.

6. Annual Review of incidents will be sent to Paul McIntyre Schools Safeguarding Coordinator 01772 532634 at County.

*Two students send abusive texts or online messages to each other and one student reports it. Other students may be involved. Staff member decides most appropriate person is HOY. HOY then gets Network manager involved and a member of SLT. All 4 members of staff will sign the incident form and actions recorded. Final form then passed on to the e safety Champion (KW) or e safety Ambassador (CB) to make sure that the incident has been actioned, resolved and filed in a secure place.

**A student comes forward worried about some indecent images they sent to a person they met online. Staff member decides that most appropriate person is e safety Ambassador. Ambassador then gets Child Protection Officer involved. All 3 members of staff will sign the incident form and actions recorded. Final form then passed on to the e safety Champion (KW) or e safety Ambassador (CB) to make sure that the incident has been actioned, resolved and filed in a secure place.

BPSC Student e Safety Incident Form

Date	
Pupil(s) involved	
Details of Incident	
Member of Stay Safe Committee recording Incident	
Member of Staff receiving student e safety incident form.	
Does a Staff e Safety Incident Form need to be filled in as a result of this form? If so, staff listed above fills in form and attaches this form to it.	
Has the incident been actioned and resolved? If yes, file form in secure place.	E safety champion or ambassador to sign below.

How do I Report an E safety Incident that happened at home or in school?

1. Collect a Student E Safety Incident Form from the
    a. school office
    b. form tutor
    c. e safety ambassabors
    d. HOY
    e. Network manager
    f. any member of the ICT & Computing Department
    g. or download the form off the e safety section of the school website

2. You may fill this form out yourself or you may ask for help from an e safety ambassador in your year.

3. When the from is complete, pass it on to the most appropriate person or who you feel most comfortable:

    a. E safety Ambassadors which are
        i. Year 7: Jasmine Garrett & Luke Abram
        ii. Year 8: Beth Andrews & Josh Herbert & Josh Wyke
        iii. Year 9: Hannah Mooney & Sean Johnson
        iv. Year 10: Ben Mawdsley
        v. Year 11: Sam Jeffries
    b. Class Teacher
    c. Form teacher
    d. HOY
    e. Network Manager (Mr Frain)
    f. Staff E safety Ambassador (Mrs Blundell)
    g. Staff Child Protection Officer and E Safety Champion (Mrs Walton)