Whitefield Primary School

E-Safety Policy

January 2012

The implementation of this policy will be monitored by Mrs Sarah Foster and Mr Simon Phillips

This policy will be reviewed as appropriate by Mr Simon Phillips

Approved by S Foster (Headteacher) Date 7 February 2012

Approved by Michael W (Governor) Date 7 February 2012

Policies/E-Safety/Created February 2008

Revised January 2012

Contents

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our school's vision for eSafety

At Whitefield Primary school, we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology, is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our eSafety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view eSafety education as a key life skill.

Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. The role of the school’s eSafety Champion

Our eSafety Champion is Mrs Sarah Foster

The role of the eSafety Champion in our school includes:

- Taking operational responsibility for ensuring the development, maintenance and review of the school‟s eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools‟ ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school‟s Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.

4. Policies and practices

This eSafety policy should be read in conjunction with the following other related policies and documents:

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

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

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Sensitive data (names, contact details, assessment data, images) should only leave the school site under password protection.
- Sensitive data should be saved in school in the designated area. This will include images, contact information for children, parents and staff, and also IEPs and assessment data.
- The School Business Manager will be ultimately responsible for managing information.
- All staff who have access to personal data should be aware of their legal responsibilities detailed in the Data Protection Act (1998).
- Only approved means should be used to access, store and dispose of confidential data.
- Any remote access of school data should be done over a secured network.
- All important data should be backed up on a daily basis.

Clear desk and screen policy

Paper and computer media are stored in suitable locked cabinets were appropriate. Sensitive printed material is cleared from printers immediately and shredded/disposed of by any staff member. Business critical information is held in a fire resistant safe or cabinet, with copies being back up off site.

PCs and printers are not left logged on when unattended and are protected as appropriate by passwords when not is use. Users terminate active sessions and log off when finished.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- Staff should be aware that some mobile devices may be able to access unfiltered internet content.
- Devices should be virus checked before linking with school systems.
- If a child brings a mobile device into school it should be kept in the designated area until home time.
- Using mobile devices to take photographs in school is actively discouraged.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), we must have written permission for their use from the individual and/or their parents or carers.
- Permission to use images will be obtained on an one of basis when the child enters the school.
- Images of pupils who have left Whitefield will only be retained for a maximum period of one year. This time period is made explicit to parents/carers.
- Full names and personal details will not be used on any digital media, particularly in association with photographs.
- When parents and carers are allowed to take videos and photographs, they are made aware of conditions in advance. The conditions are that the videos and photographs are for personal use only, and should not be posted online in any way.
- Staff are made aware of the risks of publishing images, particularly in relation to the use of personal Social Network sites.
- Photographs and videos of school activities should only be taken by staff using school equipment, and only for school purposes.
- Any photographs/videos of school activities are kept on site, or under password protection, so they can only be accessed by the appropriate staff/pupils.
- No images of school activities involving children should be kept on personal equipment. Any images of school activities involving adults should only be kept on personal equipment with the explicit consent of all the adults involved.
- When taking photographs/video, staff should ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- Guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored and reviewed by the safety champion on an annual basis.

4.4 Communication technologies

All digital communications should be professional in tone and content.

Email:

In our school the following statements reflect our practice in the use of email.

- All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
- 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. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are 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 users are 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 users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school will include a standard disclaimer at the bottom of all outgoing emails (see example below).

Example school e-mail disclaimer:

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 Whitefield Primary School. 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 Networks:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users" content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- All staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.

- Pupils must not be added as “friends” on any Social Network site.
- Whatever means of communication staff use, they should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- The school allows staff to bring in personal mobile telephones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a current pupil or parent/carer using their personal device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children. Staff bags should be placed in a stock cupboard or other suitable cupboard unless instructed by the Headteacher to move them to another appropriate location.
- With the consent of the Headteacher a member of staff may use a smart phone to support lessons.
- Mobile phone calls may only be taken at staff breaks or in staff members’ own time and in the designated staff area.
- If staff have a personal emergency they are free to use the school’s phone or make a personal call from their mobile in the designated staff areas, i.e. staffroom, PPA room, Acorn Meeting room.
- If any staff member has a family emergency or similar and required to keep their mobile phone to hand, prior permission must be sought from the Headteacher and the mobile phone be kept on silent mode in a pocket.
- All volunteer helpers/students will be requested to place their bag containing their phone in an appropriate location and asked to take or receive any calls in the staffroom.
- Visiting contractors/professionals will be informed of the school’s policy and asked to refrain from using mobile devices whilst in the school, or directed to the designated area.
- During group outings nominated staff will have access to the school’s nominated mobile phone, which is to be used for emergency purposes only.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.
- Concerns will be taken seriously, logged and investigated appropriately.
- The Headteacher or Deputy in her absence reserves the right to check the image contents of a member of staffs mobile phone should there be any cause for concern over the appropriate use of it.
- Should inappropriate material be found then the Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the staff member’s dismissal.

Instant Messaging:

Instant Messaging, e.g. MSN, Skype, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in “real time” using text, sound and video. The Lancashire Grid for Learning filtering service “blocks” these sites by default, but access permissions can be changed at the request of the Headteacher.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- Instant messaging sites should only be unblocked for strictly supervised use within the classroom setting, with staff aware of the risks involved eg: accidental viewing of inappropriate images/language.
- The secure messaging, forums and chat facilities within moodle (vle) can be used but must be monitored by the teacher who has set them up.

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- Any communication tools that are set up by a teacher (eg: discussion forums, chat sessions) must be monitored by that teacher.
- Before children use communication tools within moodle, they must first be taken through the acceptable use policy in conjunction with the eSafety curriculum.
- Pupils have access to their own year group’s area. Teachers have admin rights to their own year group area plus the staff area. Parent’s can request a username and password to access the parent’s area and their child’s year group area.
- Passwords are issued when the child starts school. For KS1 children, it is recommended that the password is uniform for the class, with no communication tools used. For KS2 children, it is recommended that they choose their own, safe, password.
- The accounts of pupils who have left the school will be deleted. For year 6, this will be in the September after they have left.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of School Websites and other online school publications:

- The school website and online publications will be consistent with the eSafety messages communicated to parents/carers and pupils.
- The use of digital media on the school website and online publications will follow the guidelines contained in section 4.3 of this policy.

- The use of personal information on the school website and online publications will follow the guidelines contained in section 4.1 of this policy.

- The school business manager has access to edit the school website. Other members of staff may be given access to edit the school website at the discretion of the business manager.

- The school website and online publications will not contain material, without consent, that is subject to copyright/personal intellectual copyright restrictions.

- The school website is available for anybody to see, and will therefore not contain any data or images that might be considered sensitive.

- Downloadable materials will be in a read-only format (eg: PDF) to prevent content being manipulated and potentially re-distributed without the school's consent.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- A permission letter will be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children will not be appearing 'live' on the Internet through a video conferencing link. However, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.
- 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.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

4.5 Acceptable Use Policy (AUP)

The following is the Acceptable Use Policy (AUP) for staff and governors.

ICT Acceptable Use Policy (AUP) – Staff and Governor

Agreement

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with pupils and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of ICT Curriculum Leader or school business manager (Admin Server).
name>.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users‟ data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
18. I will take responsibility for reading and upholding the standards laid out in the AUP.

I will support and promote the school‟s eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
19. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

The following is the Acceptable Use Policy (AUP) for Supply Teachers and Visitors/Guests.

ICT Acceptable Use Policy (AUP) – Supply Teachers and Visitors/Guests Agreement

For use by any adult working in the school for a short period of time.
1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will respect copyright and intellectual property rights.
4. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
5. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
6. I will not install any hardware or software onto any school system.
7. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

The following is the Acceptable Use Policy (AUP) for pupils.

ICT Acceptable Use Policy (AUP) - Pupils Agreement / eSafety Rules

These rules are a reflection of the content of Whitefield Primary School’s eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others’, details such as names, phone numbers or home addresses.

- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……………………………………………………….…… Parent/ Carer Signature

We have discussed this Acceptable Use Policy and ……………………………......... [Print child"s name] agrees to follow the eSafety rules and to support the safe use of ICT at Whitefield Primary School.

Parent /Carer Name (Print) ….………….. Parent /Carer (Signature) …….……..……………….

Class …………………………………………………. Date……………………..………………

4.6 Dealing with incidents

Any breach of the Acceptable Use Policies will need to be dealt with in the appropriate way, depending on the incident and who has breached the AUP. An incident log (see Appendix 10) will need to be completed to record and monitor offences. This must be audited on a regular basis by the eSafety Champion or other designated member of the Senior Leadership Team.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 11). Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Examples of illegal offences are:
Accessing child sexual abuse images
Accessing non-photographic child sexual abuse images
Accessing criminally obscene adult content
Incitement to racial hatred
More details regarding these categories can be found on the IWF website.
(http://www.iwf.org.uk)

Inappropriate use
It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions

are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent "accidental" offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

5. Infrastructure and technology

Internet content filtering is provided by default as we subscribe to the Lancsngfl/CLEO Broadband Service. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates.
Further information can be found at www.lancsngfl.ac.uk/esafety .

Pupil Access:

Children should only access school ICT equipment and online materials when supervised by a trusted adult.

Passwords:

- All users who have access to areas of the school network that contains sensitive data should have a secure username and password.

- The administrator password for the school network is available to the Headteacher and ICT Subject Leader.

- Staff and pupils should be regularly reminded of the importance of keeping passwords secure.

- Passwords will be changed every six months.
- Passwords should be a mixture of numbers and letters.

Software/hardware:

- All software used by school should have the correct permissions and licenses for it to be used legally.
- An up to date record of appropriate licenses will be kept by the school business manager and ICT subject leader.
- Software will be evaluated in consultation with the ICT subject leader before it is installed on school systems.

Managing the network and technical support:

- Servers, wireless systems and cabling are securely located and physical access restricted.
- All wireless devices have their security enabled.
- Wireless routers are accessible only through a secure password.
- Access Area are responsible for managing the security of your school network, in consultation with the Headteacher and ICT subject leader.
- The safety and security of your school network is reviewed annually.
- Computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password and permissions are assigned dependant on their position in the school.
- Staff and pupils are required to lock or log out of a school system that contains sensitive data when the computer/digital device is left unattended.
- Users are allowed to download executable files and install software, but must take care when doing so, and if in any doubt, consult Access Area or the ICT subject leader before doing so.
- Users should report any suspicion or evidence of a breach of security to the eSafety champion.
- Staff may use mobile memory devices as long as they ensure the pen drives are encrypted and are used on school ICT equipment only, therefore ensuring they have undergone a virus check, What is your school's guidance on using removable storage devices on school e.g. encrypted pen drives?
- School equipment is for the use of school staff only and should not be used by other members of the staff's family. Devices used in school that are not school property should not contain personal data.
- Any network monitoring that takes place is in accordance with the Data Protection Act (1998). Staff are made aware of all network monitoring and/or remote access that takes place and by whom.

- All internal/external technical support providers are aware of our schools requirements / standards regarding eSafety.
- The Headteacher/ICT subject leader are responsible for liaising with/managing the technical support staff.

Filtering and virus protection:

- Our school has devolved control over the LGfL filtering service.
- The filtering is managed by the ICT subject leader in consultation with the Headteacher.
- Where is information regarding devolved filtering stored in school? This needs to be available for any new member of the SLT.
- How is devolved filtering communicated to members of staff? Are staff aware of the procedures for blocking and unblocking specific websites?
- ALL equipment, including school laptops used at home, are regularly updated with the most recent version of virus protection software used in school. This will be done on a termly basis, with staff making laptops available for Accessarea to update if necessary.
- If staff suspect they have detected a virus, this should be reported immediately to the ICT subject leader who can then contact technical support.

6. Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The three main areas of eSafety risk that our school needs to be aware of and consider are:

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus', Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism

	User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

6.1eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. Our school needs to provide suitable eSafety education to all pupils and consider the following points:

- We should provide regular, planned eSafety teaching within a range of curriculum areas (using the Lancashire ICT Progression document).
- eSafety education should be differentiated for pupils with special educational needs?
- Pupils should be made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications.
- Pupils should be made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g. by using peer mentoring or worry boxes.
- Pupils should be taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- Pupils should develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils should be reminded of safe Internet use e.g. classroom displays, e safety rules, acceptance of site policies when logging onto the school network/Virtual Learning Environment.

6.2eSafety – Raising staff awareness

- All staff are expected to promote and model responsible use of ICT and digital resources.
- All staff will be regularly updated on their responsibilities as outlined in our school policy.
- The eSafety champion will provide advice/guidance or training to individuals as and when required.
- The members of staff delivering eSafety training will have received external eSafety training/updates from a county provider/CEOP.
- eSafety training will ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- eSafety training will be provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy.
- Regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

6.3eSafety – Raising parents/carers awareness

“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.” (Byron Report, 2008).

Our school will offer regular opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies.
This will be done through:

- School newsletters, homework diaries, Website, VLE/Moodle and other publications.
- Bespoke Parents eSafety Awareness sessions (one per year, on various days and times, cluster sessions).
- Promotion of external eSafety resources/online materials.

6.4eSafety – Raising Governors’ awareness

Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, will be kept up to date. This will be through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.
NB: The eSafety Policy should be regularly reviewed and approved by the governing body.

7 Standards and inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.

- eSafety incidents are recorded in the eSafety incident log and monitored and reviewed on a half-termly basis by the eSafety champion.
- The introduction of new technologies are risk assessed.
- These assessments are included in the eSafety Policy.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children. These patterns are addressed in various ways, depending on the incident and people involved e.g. working with a specific group, class assemblies, reminders for parents.
- The monitoring and reporting of eSafety incidents will contribute to changes in policy and practice.
- Staff, parents/carers, pupils and governors are informed of changes to policy and practice through staff meetings, training, lessons and newsletters.
- The AUPs are reviewed annually and they include reference to current trends and new technologies.