Westhead Lathom St. James

C.E. Primary School

eSafety Policy

"Christian values are implicit in all that we do"

Last Reviewed Date: Summer 2017

Next Review Date: Summer 2018

Version	Date	Author/Editor	Revision Notes
V 1.0	11th March 2006	Alison Albion	Original Policy documents copied into new format, with header, footer and version control.Policy reviewed and updated to ensure reflects current policy and practice
V2.0	September 2009	Alison Albion	Policy reviewed and updated e.g. to include references to emerging technologies/social networking to comply with BECTA guidelines.
V3	May 2012	Alison Albion/Alison Craven	Policy converted from old internet use policy & rewritten based on Lancashire esafety framework.
V4	January 2014	Andrew Hunt/Alison Albion/Alison Craven	
5	Spring 2015	Andrew Hunt/Alison Albion/Alison Craven	
6	Spring 2016	Andrew Hunt	

Signed.....Chair of Governors

Date.....

Mission Statement: Our School Now

Our school provides a secure, caring, stimulating and challenging indoor and outdoor environment that promotes a love of learning. Our children, parents, families, staff, governors and community work together to enable each child to become a happy, healthy, well-balanced individual in preparation for the opportunities, responsibilities and experiences of life.

The ethos of the school is based on the Christian ideals of commitment, responsibility and respect and love for Jesus Christ, self and others. We are committed to working in partnership with all of those involved in our children's development to lead our children towards tolerance, understanding, justice, and sensitivity to the needs of others and appreciation of the world around them.

Our motto "Enjoy, Respect, Learn, Achieve"

Vision Statement: Our Vision for the Future

- To provide role models who: go the extra mile; give of themselves and their time to meet the needs of the whole child; promote spirituality and an appreciation of the wonders of the natural world; promote a love of learning; develop Christian ideals of commitment, responsibility, respect, team-work, tolerance, understanding, justice, sensitivity of self and others and love for Jesus Christ, within a secure, caring, inspiring, stimulating and challenging environment both indoors and outside.
- For children, parents, families, staff, governors and community to work together in partnership to enable each child to become a happy, healthy, well-balanced individuals with self-confidence and belief that builds character to enable them to engage thoroughly, fulfilling each individual's potential through life's experiences, opportunities and responsibilities in a rapidly changing world.

Aims

Westhead Lathom St. James Church of England Primary School aims to :-

- Provide a broad and challenging curriculum and a stimulating learning environment that extends outside the classroom;
- Develop enquiring minds and spirituality through curiosity, awe and wonder of the world;
- Teach, demonstrate and praise Christian Values;
- Value the power of prayer;
- Teach with innovative and investigative approaches to learning;
- Provide an enriching programme of extra-curricular activities and visits;
- Plan a rich, varied and up-to-date range of learning resources;
- Encourage children to achieve their highest standards in all areas of the curriculum and to seek excellence within an ethos of support, challenge and encouragement to succeed;
- Teach children to work independently, collaboratively and become highly motivated lifelong learners;
- Include opportunities for creative thinking in problem solving settings, developing divergent thinking, adaptability and flexibility in preparation for the many changes ahead in life, including the rapid progress in technology;
- Build partnerships between the school, home and community;
- Strive for continuous improvement in all that we do;
- Continually self-evaluate and continue to improve upon current practice;
- Work collaboratively towards common goals;

- Place self-esteem and a positive and inclusive approach to behaviour as high priorities thus ensuring that individuals respect and value themselves, others and the environment and is motivated to do their best in school and beyond in order to become a fulfilled adult who gives to the community.

Contents

1. Introduction

Policy Scope

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors, trainee teachers, volunteers and school community users).
This E-Safety policy has been developed by a working group made up of

- Headteacher
- Online Saftety Coordinator
- Staff – including Teachers and Support staff
- Governors
- Pupils (Online Safety Group)

E-Safety Risks

This policy adresses the following risks which have been identified in Becta's Safeguarding Children in a Digital World Advice Document;

E-Safety Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse

E-Safety Contact

- Grooming using communication technologies, leading to sexual assault and/or child prostitution

E-Safety Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

E-Safety Culture

- Bullying via websites, mobile phones or other forms of communication device
- Downloading of copyrighted materials e.g. music and films

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.

Creation, Monitoring and Review

The School's E-Safety Group consists of The Headteacher, Safeguarding Officer, ICT Co-ordinator and The Chair of Governors. Consultation with this group was carried out before the policy was approved.

The impact of the policy will be monitored and reviewed with a full review by the E-Safety group to be carried out once a year. The policy will also be reconsidered where concerns are raised by The Safeguarding Officer or when an e-safety incident has been recorded.

The Group will do all that it can to make sure the Group's network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of systems and information.

2. Westhead Lathom St. James C.E. Primary School's vision for eSafety

Westhead Lathom St. James C.E. Primary School provides a diverse, balanced and relevant approach to the use of technology.

- The school recognises the use of the internet in the 21st Century as a tool to raise educational standards, to promote pupil achievement and as a tool for staff to enhance the learning opportunities for children.
- Internet access is therefore an entitlement for pupils who show a mature and responsible approach to use it.
- Staff should guide pupils in on-line activities that will support learning.
- The schools internet has been designed for pupil use and is filtered appropriate to the age of the pupils.
- The school has subscribed to a variety of online programs (Mathletics, Spellodrome, Purple Mash and Espresso) which the children can access outside of school. They will therefore need to learn how to take care of their own safety and security.
- The users in the school community understand why there is a need for an eSafety Policy.
-

3. The role of The Online Safety Group

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governors has taken on the role of Online Safety Governor. The Governor will have regular meetings with the Online Safety Co-Ordinator and they will regularly monitor the Online Safety Incident Log.

Headteacher
The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The Headteacher is responsible for ensuring the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues.

Pupils
Every class will included children who have been designated as 'Online Safety Experts'. This group of children will meet regularly with The Online Safety Coordinator to discuss aspects of online safety. They will have the knowledge to ensure that any online safety concerns are dealt with correctly in the classrooms and reported to a responsible adult. They will also lead by example and show other children how to use the internet safely. At certain points in the year, the online safety group will create presentations and take school assemblies to teach children about online safety.

Online Safety Co-ordinator
The role of the eSafety co-ordinator includes:

- Having 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
- Liaising with parents in order to be aware of any eSafety Incidents at home which could affect children at school too.
- 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).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- 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.

4.

5. Policies and Practices

Security

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

Schools ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly.

Equipment

School equipment, including teacher laptops, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Staff laptops are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported to the safety coordinator.

School equipment must not be used , for example for online gambling, dating websites, home shopping, booking holidays, social networking both at home and in school.

Protecting Personal Data

Staff are aware of the school's procedures for disposing of sensitive data eg shredding hard copies, deleting digital information, deleting email accounts/moodle usernames & passwords, IEP, PIPs, SATs information. All of this information will be stored on main office computer and teachers personal laptops only. No sensitive or confidential information is to be put on class laptops. The school's Safeguarding Officer is responsible for managing this information.

School data must not be stored on personal equipment e.g. home computer or mobile phone. The school's procedure for backing up data is on discs which are replaced on a daily basis with one copy always kept off-site.

Staff have been provided with training on the storing information during Spring 2014. Staff can access Lancashire NGFL for storage via the secure username and password provided by school. Teachers also use 'dropbox' via their approved email address to secure day to day resources.

Publishing Pupils' Images and Work

Parents will be asked to sign a consent form before pictures of pupils are published either via the school website or the school newsletter. Photographs that include pupils will be selected carefully and pupils' full names will not be used anywhere on the Web site particularly in association with photographs. Work can only be published with permission of the pupils and parents.

4.1. Use of mobile devices

The school now uses a range of mobile devices to extend children's learning. Currently the children have access to laptops, beebots, probots, cameras and tablets.

Mobile Devices

The class teacher is responsible for mobile devices for his/her classroom such as beebots, probots and cameras. Only school cameras may be used to photograph children and their work. These images will only be stored on the password protected class laptop which is also the responsibility of the class teacher. In some cases the teacher may require children to take images an use them on class laptops as part of a learning opportunity. In this instance staff will supervise children at all time and clear instructions will be provided to the children to ensure the images or videos are not used inappropriately.

Many of the E-Safety issues that apply to the use of iPads already exist within school and have been addressed in our E-Safety Policy. All teachers currently have access to an ipad which are used for class teaching or on a 1:1 basis with pupil. As of Spring 2014 the school has invested in ipads which are to be used on a wider scale by the children. It is therefore important that their acceptable use is properly addressed. Before being allowed to use the ipads all staff and pupils should have received and signed a copy of the ICT Acceptable Use Policy.

The camera's on the ipads may be used but only at the teachers discretion. This images must not be directly uploaded to the internet by staff or pupils. They must first be put on a teachers laptop and approved by staff, parents and pupils.

Any use of email on ipads should be closely monitored by teachers and staff. The class ipads will not be linked to a school email so children cannot access this feature. However since email has now become a key means of communication the teacher may wish to allow temporary access to email but only via an approved school email address so that its used can be closely monitored.

Mobile Phones

Children are not permitted to bring mobile phones into school. Adults in school may use mobile phones during non-directed time to make personal calls. Non-directed time includes: before school, at lunch-time and after school. Adults should not text or call during lessons/activities where they have a supervisory role. Should a member of staff need to be reached, the most effective method is through calling the school office.

Adults **must not** give out mobile phone numbers to parents on field or residential trips but instead should provide the school office number. The school office will then contact the teacher or member of staff involved.

At no point should a personal mobile phone be used to record images (photograph or video) of a child or children. Instead, if an image or video is needed, a school digital camera must be used.

Children should not bring other personal mobile devices such as games consoles and tablets into school.

4.2. Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure, local newspaper reports or display.

- At school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers.
- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used. The parental/carer permission is obtained in reception but the parents have a right to change this if deemed necessary (see Appendix 1: image consent form)
- A list of children whose parents have not given permission for use of images is stored in the school office & in each classroom. This has particular significance when dealing with photographs for inclusion in newspaper articles as they often require full names.
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs (unless photographs are to be part of a newspaper article celebrating school events & parental permission has been obtained).
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are encouraged not to store digital content on personal equipment.
- Staff are encouraged not to use their own cameras.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils made aware that images of pupils or adults can be published on the internet in any form, including Social Network sites, without the consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the Headteacher and Governors on an annual basis.

4.3. Communication technologies

As a school we understand the importance of communication and the role it plays in today's society and endeavour to educate and protect the children in our care.

Email

- All users have access to the Lancashire Grid for Learning service as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.
- The Lancashire Grid for Learning filtering service reduces 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.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Bebo 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.

All staff need to be aware of the following points:

- They 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.
- Children who are under 13 are not legally allowed to members of Facebook.

Remember; whatever means of communication you use you should always conduct yourself 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

- The school allows personal mobile phones to be used in school by staff and visitors but are asked to be left on silent in curriculum time.
- It is acceptable to use personal mobile phones for school activities e.g. school trips.
- Pupils are not permitted to bring mobile phones into school. If they are brought into school by mistake or are required for the journey to and from school, they must be stored in the school office until the end of school.

Texting

Westhead Lathom St. James C.E. Primary School subscribes to 'teachers2parents to communicate messages to parents/carers & staff via text. This is accessed via a secure website. Access to the password is limited to the Headteacher/class teachers and school admin officer. Messages must be limited to relevant school messages e.g. football cancelled, homework due in tomorrow. This system should not be used for personal messages.
Access must be between the hours of 8.00a.m. and 6.00 p.m. unless it is an emergency e.g. school closures.

Virtual Learning Environment (VLE) / Learning Platform

School has chosen to use Moodle as a communication tool.

- All children will be given access to the Moodle but teachers have access to all accounts
- Passwords are issued to the children and they are encouraged not to share their password
- Pupils are taught to use these communication tools in a responsible way in conjunction with the eSafety curriculum.
- Teachers know how to monitor the use of the Moodle with their class.
- Accounts are deleted when staff and pupils leave the school. This is monitored by the ICT coordinator

Web sites and other online publications

This may include for example, podcasts, videos, 'Making the News' and blogs.

- The school website is effective in communicating eSafety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media and personal information on the website.
- Teachers have access to edit the school website.
- All users are aware of copyright restrictions including personal intellectual copyright and will not publish anything that does not meet this.
- The Head teacher has overall responsibility for what appears on the website.
- Any file available for download is in PDF file to eliminate manipulation and redistribution without consent.

Video Conferencing

- Videoconferencing should use the educational broadband network to ensure quality of service and security
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Others
The School will adapt/update the eSafety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

4.4. Acceptable Use Policy (AUP)

Our Acceptable Use Policies (See appendices 2 – 4) are intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.
AUPs are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.
Our school AUPS aim to:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
    - Cyberbullying
    - Inappropriate use of email, communication technologies and Social Network sites and any online content
    - Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.5. Dealing with incidents

At Westhead Lathom St. James C.E. Primary School an incident log (see appendix 7) is completed to record and monitor offences. This is audited on a regular basis by the eSafety co-ordinator or Headteacher

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. Any potential illegal content would be reported to the Internet Watch Foundation (http://www.iwf.org.uk). They are licensed to investigate – schools are not! (See Appendix 8).

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 the 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 proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied.

Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident Procedure and Sanctions

Incident	Response
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 coordinator. ○ 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.	

- The Headteacher is responsible for dealing with eSafety incidents. All staff are aware of the different types of eSafety incident and how to respond appropriately. e.g. illegal or inappropriate.
- Procedures are in place to deal with eSafety incidents and all staff aware of these.
- Children are informed of the procedures through discussions with members of staff.
- These incidents are logged in a log book kept in the office. (See Appendix 7)
- Incidents are monitored, by the headteacher on a regular basis.
- The measures that are in place to respond to and prevent recurrence of an incident.
- The Headteacher will decide at which point parents or external agencies are involved

- The procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member (Appendix 8)

The school uses the 'eSafety Incident/ Escalation Procedures' document (See Appendix 8) as a framework for responding to incidents.

6. Infrastructure and Technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided by the Lancashire Grid for Learning.

Pupil access

The children are supervised by staff when accessing school equipment and online materials

Passwords

- All staff aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at www.lancsngfl.ac.uk/esafety website.
- Our curriculum network does not need password access. All Moodle users have passwords which are kept within Moodle and only the Headteacher/class teachers & admin officer have access to these. Children and staff are reminded of keeping them secure whenever they use them.
- The password for the admin network is available to the Headteacher and admin officer
- Staff and pupils are reminded of the importance of keeping passwords secure

Software/hardware

- All software is licensed or free to download/use. Licences are kept in a secure place in the school office and the ICT co-ordinator is responsible for maintaining this.
- Users are allowed to download software with the permission of the ICT coordinator who ensures correct licences are obtained.

Managing the network and technical support

- Wireless systems and cabling are securely located and physical access restricted.
- All devices that access the wireless management system have security enabled and can only be accessed with the schools wireless network password. The ICT coordinator is responsible for managing the security of the school network.
- The safety and security of the school network is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users report any suspicion or evidence of a breach of security to the ICT coordinator
- The school encourages staff not to use removable storage devices on school equipment e.g. encrypted pen drives.
- The school encourages teachers to follow esafety policy guidelines when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with the Data Protection Act (1998)

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

Filtering and virus protection

Westhead Lathom St. James C.E. Primary School uses the LGFL filtering service for any online activity. If there is a particular problem with a site or the need to unblock a site then the Headteacher will liaise with LGFL to try to remedy the problem. Virus protection is supplied by Sophos in conjunction with LGFL. Staff laptop must have Sophos installed & automatic updating enabled.

7. Education and Training

In 21st Century society, 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 main areas of eSafety risk that we need to consider:

Area of Risk	Example 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.

6.1. eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. As a school our approach to learning is through a creative curriculum that uses strong cross-curricular links between subjects. We see eSafety as reaching across all subjects and is therefore addressed initially through ICT and PHSE but then reinforced through all other

subjects. Westhead Lathom St. James C.E. Primary School provides suitable eSafety education to all pupils:

- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are
- affected by these issues, e.g. using peer mentoring.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils 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.
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules (See Appendices 2 - 4).
- We have a dedicated focus in collective worship every year using Barney & Echo materials.

6.2. eSafety – Raising staff awareness

- Regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.
- The eSafety co-ordinator provides advice/guidance or training to individuals as and when required.
- The eSafety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Esafety training is 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.

6.3. eSafety – 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).

The school offers opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies. For example through:

• School newsletters, Website, VLE/Moodle and other publications.
• Promotion of external eSafety resources/online materials.

6.4. eSafety – Raising Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

7. Standards and Inspection

At Westhead Lathom St. James C.E. Primary School:

- E-Safety incidents are monitored, recorded and reviewed.
- The Headteacher is responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is 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 would be addressed most effectively by e.g. working with a specific group, class assemblies, reminders for parents.

8. List of Appendices

Appendix 1: Use of Images

Dear Parents,

Occasionally, we may take photographs of the children at our school. These images may be used in our school prospectus, in other printed publications that we produce, on our school website, or on project display boards in school. Very occasionally, we may be visited by the media who will take photographs or film footage of pupils (eg at a high profile event, to celebrate a particular achievement etc.) Such images may appear in local or national newspapers, or on televised news programmes.

In order to comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Equally, we are committed to continue to work closely with parents in an attempt to take all reasonable steps towards making the school environment as safe as possible.

Please answer questions 1-4 below before returning the completed form (one for each child) to school as soon as possible.

		(Please tick)	
1.	May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes, or on project display boards?	☐ Yes	☐ No
2.	May we use your child's image on our school website?	☐ Yes	☐ No
3.	May we record your child's image on video?	☐ Yes	☐ No
4.	Are you happy for your child to appear in the media as part of school's involvement in an event?	☐ Yes	☐ No

Please note, in order to be published in the press it is often necessary to include your child's full name.

I have read and understand the conditions of use attached to this form.

Signature of Parent or Guardian ……..

Name ……..

Date ……..

Appendix 1: Use of Images

CONDITIONS OF USE

1. This form is valid for the period of time your child attends this school/. our consent will automatically expire after this time

2. The school will not re-use any photographs or recordings *after your child leaves this school.

3. The school will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image, on video, on our website, in the school prospectus or in any of our other printed publications

4. The school will not include personal e-mail or postal addresses or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

5. If we use photographs of individual pupils, we will not use the name of that child in any accompanying text or caption unless it is required for publication in a newspaper article.

6. If we name a pupil in the text, we will not use a photograph of that child to accompany the article unless it is required for publication in a newspaper article.

7. We may include pictures of pupils and teachers that have been drawn by pupils.

8. We may use group or class photographs or footage with very general labels, such as 'a science lesson'

9. We will only use images of pupils who are suitably dressed

10. Parents who are invited to attend events where photography/video recording is permitted by them in school should undertake to ensure that any images or materials produced are for family/private use only.

11. Parents should note that websites can be viewed throughout the world

12. We undertake to take all reasonable steps to ensure that any images maintained in school are stored securely and are accessed only by authorised persons

Mrs A. Albion

Headteacher

Appendix 2

ICT Acceptable Use Policy (AUP):
Staff & Governor Agreement

ICT and the related technologies such as email, 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.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- 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.
- I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- 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.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I will ensure that all electronic communications with pupils and other adults are appropriate.
- I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)
- I will not install any hardware or software without the prior permission of the ICT coordinator
- 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.
- 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.
- I will report any known misuses of technology, including the unacceptable behaviours of others.
- 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.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
-

Appendix 2

ICT Acceptable Use Policy (AUP): Staff & Governor Agreement

- 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.
- I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
- 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.
- 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.
- 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.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

Full Name …… (PRINT)

Position/Role ……

Appendix 3

ICT Acceptable Use Policy (AUP)

Pupils Agreement / eSafety Rules

These rules are a reflection of the content of our 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 email 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 Westhead Lathom St. James C.E. Primary School

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class …… Date……

Appendix 4

ICT Acceptable Use Policy (AUP) – Parents' Letter

Dear Parent/ Carer,

The use of ICT including the Internet, email, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour Policy outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read an discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

If you would like to find out more about eSafety for parents and carers, please visit the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact *Mrs. Albion*

Yours sincerely,

Mrs Albion
Headteacher

Appendix 5

eSafety Rules: EYFS/KS1

These rules help us to stay safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Appendix 6

eSafety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programs and content which have been installed by the school.

Appendix 7

eSafety Incident Log

All eSafety incidents must be recorded by the School eSafety coordinator or designated person. This incident log will be monitored and reviewed regularly
by the Headteacher and Chair of Governors. Any incidents involving Cyberbullying should also be recorded on the 'Integrated Bullying and Racist Incident Record Form 2' available via the Lancashire Schools' Portal.

Date / Time of incident	Type of Incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)

APPENDIX 8 – Responding to eSafety Incident/ Escalation Procedures