Lea Endowed CE Primary School

Online Safety Policy

Approved by: Governors
Updated: January 2019
Review: January 2021 or sooner if needed.

Our School Mission Statement
At Lea Endowed Church of England School we are committed to providing an excellent education for our children. We seek to follow God's example to love Him, and each other, in all that we do. Our whole school family is encouraged to achieve their full, God given potential and shine in their own special way.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1. The Technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside school, by children include:

- E-mail, Hotmail, Gmail
- The Internet
- Instant messaging, Viper, WhatsApp, Skype, Instagram, FaceTime, often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.instagram www.OOvoo www.snapchat /http://www.twitter.com/ http:www.facebook.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular Xbox / PlayStation, I messages, Oromo)
- Gaming Sites (Popular www.neopets.com, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www-spotify.com/, http://www.deezer
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Tablets/I pads/e-Readers/Mod books/Kindles and other such technologies which are 'internet ready'

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- A range of technological tools including Laptops, computers, I Pads, smart boards, projectors and interactive boards, digital media equipment, data logging equipment, control equipment, software.
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive Online Safety education programme for pupils, staff, parents and stakeholders.

3. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school. The Headteacher, with the support of Governors, aim to embed safe practices into the culture of the school. It is the responsibility of the Headteacher to ensure that the Policy is implemented and compliance with the Policy monitored.

Our school **Online Safety lead is Catherine Seagrave**

Our Online Safety Coordinator keeps up to date with Online Safety issues and guidance through liaison with the schools Computing coordinator, the Local Authority Online Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). The school's Online Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors have an overview of Online Safety issues and strategies at this school and are aware of local and national guidance on Online Safety and are updated as necessary on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and beyond and following school Online Safety procedures. This culture is embedded into the ethos of Lea Endowed School, pupils who feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' procedures for:

- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of e-mail;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as digital recording devices and digital cameras, mobile phones;
- publication of pupil information/photographs and use of website;
- e-Bullying / Cyberbullying procedures;
- their role in providing Online Safety education for pupils;

Staff are updated about Online Safety matters at least once a year.

Online Safety is included throughout the curriculum to ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

The school makes efforts to engage with parents over Online Safety matters and parents/guardians/carers sign and return an Online Safety/Acceptable Use Policy form giving permission for their child / children to access the Internet safely before any teaching begins.

4. Breaches

How will breaches be handled?

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Students:

All **pupils** should be familiar with the schools' procedures for:

Type A breach Use of non-educational sites during lessons

- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

*[Possible Sanctions: **referred to class teacher / coordinator** / senior leader / Online Safety Coordinator]*

Type B breach

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites,
- Use of File sharing software e.g. Napster, Vanbasco, LiveWire, etc.
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

*Possible Sanctions: **referred to Class teacher/ Coordinator / Member of the Senior Management Team / Online Safety Coordinator** / contact with parent*

Breaches may result in access to the internet being suspended temporarily or permanently.

Type C breach

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message, including sexting, that is regarded as harassment or of a bullying nature
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

*Possible Sanctions: **referred to Class teacher / coordinator / Online Safety Coordinator /senior leader/ Head teacher / removal of Internet use /** contact with parents*

Breaches may result in access to the internet being suspended temporarily or permanently

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site/BT Lancashire Education Services
2. Inform Local Authority
3. Inform Safeguarding Officer

Type D breaches

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

*Possible Sanctions – **Referred to Head Teacher / Contact with parents** / possible exclusion / removal of equipment / refer to Community Police Officer / LA Online Safety officer*

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender’s e-mail service provider

Staff:
All **staff** should be familiar with the schools’ procedures for:

Type A breaches (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff member’s professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

*Sanction - **referred to line manager / Headteacher**. Warning given.*

Type B breaches (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*Sanction – **Referred to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers, HR, LADO - to ensure there is no risk of pupils accessing inappropriate materials in the school
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and Students be informed of these procedures?

- They will be fully explained and included within the school's Online Safety/ Acceptable Use Policy. All staff will be required to sign the school's Online Safety Policy Acceptance Use form;

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online Safety / acceptable use form;

- The school's Online Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.

- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.

- Staff are issued with the 'What to do if?' guide on Online Safety issues, (see BT Lancashire Education Services safety site).

5. Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies but their perceptions of the risks may not be well developed; the Online Safety rules need to be explained and discussed.

Online Safety will be taught in computing lessons and as part of the PHSE programme, reinforced where appropriate across the curriculum.

Useful Online Safety programmes include:

- www.internetmatters.org, www.childnet.com, www.safeinternet.org.uk
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/
- SWGFL

The teaching of Online Safety is ongoing and taught explicitly and embedded throughout the curriculum.

- Online Safety training is part of the new national curriculum for Computing and will be used to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use will precede Internet access.
- An Online Safety module will be included in the PSHE, Citizenship programmes covering both school and home use.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administrative, premises management, governors and teaching assistants are included in appropriate awareness raising and training. Induction of new staff includes a discussion of the school's Online Safety Policy.

- Staff should be made aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school will offer to support parents to plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- A wide variety of support materials and web based advice is available for parents via school website, newsletters and meetings for parents.

5. E-mailing

Managing e-mail, how will e-mail be managed?

E-mail is now an essential means of communication for staff in schools and everyday life. Directed use of regulated e-mail in schools can bring significant educational benefits, increases the ease of communication with parents and within the school community and facilitates local and international school projects. However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate.

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively with up to date account details of users.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography and inappropriate language. Finally, and in support of these, BT Lancashire Education Services filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- We use BlueOrangeIT SURFPROTECT filtering systems.
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses through class teachers.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;

    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use Office 365 e mail systems on the school system, provided by the Education Version of Microsoft Office 365.
- Staff only use school e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX*, SIMs (LA SYSTEM)*
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;

- All staff sign our LA / School Agreement Form AUP to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Technology:

Spam, phishing (the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online) and virus attachments are all potential risks to be considered.

Filtering software must be used to stop unsuitable mail.
BlueOrangeIT filtering provision is highly efficient in this respect, although it should be stressed that the technology only forms part of the protection strategy and should not be relied upon in isolation. Instead, it should be used alongside good classroom and supervisory practices, user education, and diligent individual behaviour.

Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. Schools in Lancashire have appropriate educational, filtered Internet-based e-mail options through the Lancashire Grid for Learning (LA) and LA Securemail is used for receiving confidential information.

If you have a serious child protection issue using email you should refer this to your LA or other appropriate authority, (e.g. a child's disappearance may require investigative access).

Procedures:

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses for professional purposes, such as Hotmail, must be avoided by all staff working in schools. Staff should be required to use the appropriate LA or BT Lancashire Education Services StaffMail system for professional purposes.

Individual pupil e-mails which allow pupils to send and receive messages to and from the wider world, still need to be carefully allocated to appropriate situations. A school may not even need to use email anymore as communication can be achieved within the Learning Platform.

Many teenagers will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. These should not be used for school purposes. Where e-mail accounts are not monitored, there is the risk that pupils could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring and tracing very difficult and require support from the providers of the email system (who may be an international company).

Email must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured email system, approved and deemed appropriate for such use by your Local Authority. [you need to check with your Local Authority what their procedures are as in generally this is not acceptable practice]. It is worth knowing that the data (in emails or other systems) does not belong to the User but to the organisation and they are not authorised to do as they please with the organisation's data. Therefore, a school user could be personally liable for breaching the Data Protection Act (DPA98) if personal information was disclosed because of their unauthorised actions.
[Email practice has direct relevance to your school Information Handling / security policy and should be considered both by the School's Senior Information Risk Officer (SIRO) and the Information Asset Owner. Both these individuals should be named].

Education:

Staff and pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's Online Safety and anti-bullying education programme.

Pupils need to understand good 'netiquette' style of writing, (this links to English) and appropriate e-mail behaviour. An e-Literacy and Online Safety scheme of work with associated links is available at http://www.BT Lancashire Education Services.net/esafety/Pages/education.aspx?click-source=nav-esafety

5. How will complaints regarding Online Safety be handled?

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements/breaches in use and possible sanctions. Sanctions will include:

- informing the class teacher, phase leader and Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period
- referral to LA / Police.

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Use of digital and video images

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff will authorise the website's content and check suitability.

Use of still and moving images

Most importantly, take care when using photographs or video footage of pupils on the school website. Consider using group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

If the pupil is named, avoid using their photograph / video footage.

If the photograph /video is used, avoid naming the pupil.

Skype: FACETIME

Skype/Facetime or similar platforms should only be used with full teacher control where it is deemed appropriate/safe to enhance curriculum learning.

Blogging:

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
If showcasing examples of pupils' work consider using only their first names, rather than their full names.
Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory. If the school's website contains any guestbook, noticeboard or blog, they need to be monitored to ensure they do not contain personal details of staff or pupils.

Parent/Carer content:

Parents are asked to sign permission forms related to the publishing of photographs / video footage.

Procedures:

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.
Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

School Website:

Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

Digital images - photographs and video clips - can now readily be taken using mobile phones. Therefore, images will only be recorded/captured on approved school devices.

Misuse:

Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised. Pupils who bring mobile phones / devices into school are asked to check they are switched off and handed in to the head teacher at the start of the day and they are returned to the child at the end of the school day or after after-school club activities.

Staff are advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network/server and will not be stored at home or on memory sticks and used for any other purpose than school approved business. During school trips only school Ipads are used for recording photos or video.

Technical:

Digital images / video of pupils will be stored securely on the school network/server and old images deleted after a reasonable period, or when the pupil has left the school.

When saving pictures, we will ensure that the image file is appropriately named, not using the pupils' names in image file names.

Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.

There are safe online environments for publishing, such as the BT Lancashire Education Services portal or VLE and School 'Book Publishing' websites.

Education:

Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the Schools Bursar and/or administration officer.
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network/server and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their Online Safety education programme;

Policy - Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed, ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time ‘remote’ training support;
- secure data exchange between local and government bodies.

In support of this, the government provides a Standards Fund grant to support Local Authorities procure broadband services through local Regional Broadband Consortia (RBC). In Lancashire, CLEO is the RBC. Many Lancashire schools are connected onto this broadband network. CLEO is part of the National Education Network (NEN). All English maintained schools are expected to be part of the NEN.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a ‘No Blame’, supportive culture if pupils are to report abuse. Risks can be high outside school, so schools should consider extending an education programme to parents and carers.

Schools also need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to ‘groom’ children. The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

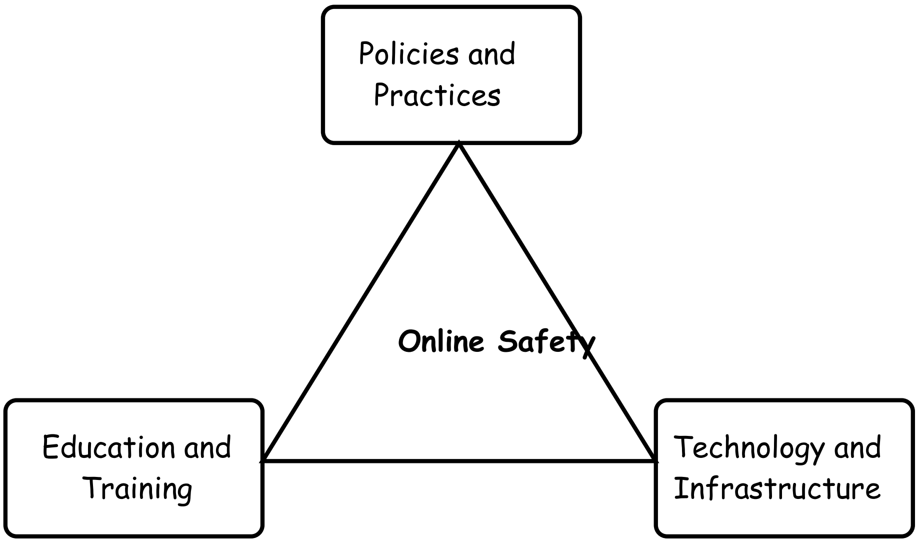
Schools help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is “unauthorized” and infringements/breaches will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff, (and parents).

There are three core elements for an institution to address when considering whole school Online Safety:

Technology

Policy and Practices

Education and training



The following pages looks at each in turn.

Technology and infrastructure: Background information

Schools should be connected to the NEN through their RBC. In Lancashire, Lea Endowed Primary School uses BlueOrangeIT who procure the broadband supply. Across this schools' fibre network, a range of services are provided. Internet filtering is a key service. This is updated and monitored by BlueOrangeIT and technical support is provided by Western.

Additionally, schools should have up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. There are BT Lancashire Education Services solutions provided for all of these and they should be set-up to be automatically updated so that networks remain up-to-date. **At Lea Endowed we use Surf Protect filters and Sophos anti-virus is provided via LCC.**

To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and pupils should not be able to download executable files and software.

Unfortunately, inappropriate materials will inevitably get through any filtering system. So, schools should be vigilant and alert so that sites can be blocked. Conversely, sometimes appropriate websites need to be unblocked. In larger schools, network managers will be able to block or liaise directly with Lancashire over this. In primary or smaller schools, there should be a named member of the Computing strategy team who manages the filtering policy for the school: this person may be the technician or the Headteacher, and the LA will usually be able to provide them with advice and back-up. By working together, Lancashire schools help to make the filtering system as effective as possible. **At Lea Endowed, the Head teacher and School Manager have the authority to / and will facilitate the blocking and unblocking of specific websites as appropriate.**

High level monitoring of website access is also undertaken by BlueOrangeIT and logs can be obtained where a site is under investigation.

Networks can have 'health' checks to ensure they have the latest versions of patches and service updates and to check speed and the possibility of having inappropriate applications on the network. This is particularly useful for secondary phase and larger schools. *[contact your LA for details]*

Filtering, coupled with child-friendly search engines [e.g. http://yahooligans.yahoo.com/ | http://www.askforkids.com/] reduce the likelihood of children finding inappropriate materials. Schools should set-up search engines so that 'safe search' is turned on: Although not a child friendly search engine, it is worth noting that Google can be forced into safe search mode through the BT Lancashire Education Services provision.

Caching some sites - so they are now essentially stored as off-line resources for viewing later from the Local Area Network (LAN) is another useful strategy. Schools may use a cache server, such as the BT Lancashire Education Services CachePilot or other LA recommended solution.

Schools should not send personal data across the Internet unless it is encrypted or sent via secure systems or an approved Learning Platform etc.

Technical and Infrastructure: suggested strategy statements

Lea Endowed:

- Maintains the filtered broadband connectivity through CLEO/Blue Orange/BT Lancashire Education Services and so connects to the 'private' National Education Network;
- Works in partnership with the LA and technical support to ensure any concerns about the system are communicated to BT Lancashire Education Services so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus software etc. and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by having LA / Blue Orange/CLEO health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with BT Lancashire Education Services services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Has *the ICT service components through BT Lancashire Services* network auditing software installed;
- Uses whole class log-ins for pupils and all other users have their own personal password protected logins
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure CLEO/BT Lancashire Education Services portal or Learning Platform.

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear.

Supervision is the key strategy and a policy that is shared and understood and reinforced by the whole school community is paramount.

Surfing the Web

Aimless surfing should never be allowed. Pupils will be taught the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'. [See Education section]

Coordinator will ensure that pupils have a limited selection of Web sites available checked by the teacher so they are appropriate for the age group and fit for purpose. Favourites are a useful way to present this choice to pupils.

Teachers' web site selections for various topics can be put onto a topic page on the Virtual Learning Environment or Lancashire VLE so pupils can, access out of school, from home etc. Some schools have put links on are put on their school web site, although there may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one. Therefore, sites should always be previewed and checked, and work for children is best located on the closed Learning Platform.

Search Engines

Some common Internet search options are high risk, for example Google image search. Some LAs and Councils block this (at a Corporate level). Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk. Talk to your network manager or LA about this. BT Lancashire Education Services guidance is available on the safety site.
[NB: Images usually have copyright attached to them.]

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcasting (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. However, schools should focus on using the social collaboration tools in the Lancashire Learning Platforms, rather than externally hosted Internet sites.

Blogs: A School may want to use them as a method of online publishing, perhaps creating class blogs, or to creatively support a specific school project. Schools should follow Local Authority advice. A 'safe' blogging environment is likely to be part of a school's future Learning Platform.

Video Conferencing
Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. [e.g the BT Lancashire Education Services nature cam and weather cams.] Webcams are also used widely for streaming video as part of a video conferencing projects.

Schools wishing to use Internet webcams outside of the BT Lancashire Education Services environment should be aware of, and follow LA.

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

Social Networking Sites
Children at Lea Endowed are not allowed access to these sites. However, pupils are taught safe behaviour as they may well be able to readily access them outside of school. There are educational, monitored services that schools can purchase such as GridClub SuperClubs. Additionally, the BT Lancashire Education Services Learning Platfom provides a safe environment for pupils to create their own webspace, store files in an ePortfolio, and communicate with others through 'closed' discussions, etc.

Podcasts
Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the BT Lancashire Education Services.

Chatrooms
Children at Lea Endowed are not allowed access to these. However, pupils are taught safe behaviour as they may well be able to readily access them outside of school.
Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms such as www.teenchat.com, www.habbohotel.co.uk, www.penguinchat.com See additionally the Becta advice.

Sanctions and infringements
The school's Online Safety / Acceptable Use policy needs to be made available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school needs to have made clear possible sanctions for infringements.
Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Policy and procedures: suggested strategy statements

Lea Endowed:

- Supervises pupils’ use at all times, as far as is reasonable, and is vigilant in learning resource areas;
- We use the CLEO / Blue Orange/ BT LANCASHIRE EDUCATION SERVICES filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed ‘safe’ environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils’ ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Coordinator / School’s Business Manager/Headteacher. Our systems administrators report to LA / BT Lancashire Education Services where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks social networking sites for specific purposes / Internet Literacy lessons;
- Only uses the BT Lancashire Education Services / NEN service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Requires pupils (and their parent/carer) from Nursery, Extended Services, Reception, Key Stage 1 and 2, to individually sign an Online Safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Uses closed / simulated environments for e-mail with Key Stage 1 pupils;
- Requires all staff to sign an Online Safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the Online Safety acceptable use agreement form at time of their daughter’s / son’s entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training programme: background information

It is a sad fact that pupils will occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. Pupils (and staff) need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or ICT manager for inclusion in the list of blocked sites.

Pupils and staff must learn to recognise and avoid risks online – to become 'Internet Wise'. To STOP and THINK before they CLICK. Both need to understand how to ensure personal information is, and remains, private. Staff must not confuse or compromise their professional role with any personal online activity, for example inviting pupils into their personal social networking site.

Pupils also need to be 'savvy' about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet – based information. Just because something is published in text or on-line does not make it fact. It's therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that pupils consider whether something is plausible or biased.

Information literacy skills therefore need to be taught. These include skills to 'read' content – (contextual clues including design, lay-out, text, and use of images, links to and from the content), where the material originates from and how the content can be validated.

More often in schools, pupils will be accessing reliable material but need to select that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including how to narrow down searches and how to skim and scan content.

The philosophy of sharing information across the Internet has increased the risk of pupils infringing copyright and committing Plagiarism (the theft of ideas and works from another author and passing them off as one's own). For older pupils, there are numerous 'essay bank' websites offering access to essays for free or for a fee, often encouraging students to submit their own works. Students should be aware of the issues around copyright and encouraged to look for copyright information on websites, so reinforcing their understanding of the importance this issue. They also need to be aware that plagiarism is not only cheating but where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

Pupils also need to understand the dangers of using unfiltered web access outside school at a location where parental controls or filtering have not been enabled. Pupils should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website, in a message or in a social networking environment.

Pupils and staff need to know how to deal with any Cyber Bullying incidents. Pupils need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), http://www.ceop.gov.uk/ – so that in an extreme case, they know how to "report abuse". See key organisation links: http://cms.BT Lancashire Education Services.net/BT Lancashire Education Services/web/safety/organisations

Where they do communicate or publish work outside of the BT Lancashire Education Services environment or other approved educational environment, it should be under adult supervision wherever possible.

Pupils and staff need to know appropriate / netiquette in their general communications:

So, to enable this, Online Safety must be built into schemes of work as appropriate, to ensure pupils are 'taught' safe behaviours and practice and the school must foster a 'No Blame' culture to ensure pupils feel able to report any abuse, misuse or inappropriate content. Key resources include the DfES/Becta Internet Proficiency Scheme at Key Stage 2 together with resources from CEOP's Think U Know site.

Parents have an important role in supporting safe and effective use of the Internet by pupils – so schools need to consider a rolling training programme of support.

See parents' resources: http://BT Lancashire Education Services.net/BT Lancashire Education Services/web/safety/resources

A wealth of Online safety links are available via the school website and are regularly referenced on Newsletters.

Education and training: suggested strategy statements

Lea Endowed:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive Online Safety education programme throughout all Key Stages, built on LA / Lancashire/ national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;

    - to understand why they must not post pictures or videos of others without their permission;
    - [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- Makes training available annually to staff on the Online Safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - distribution of ‘think u know’ for parents’ materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Managing Equipment

Using the school network, equipment and data safely

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school’s Online Safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with an individual network log-in username (currently whole class log- ons and passwords).
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- All school equipment is to stay on the school premises unless it is being using for a school visit

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  <LIST e.g. Local email or Intranet; finance system, Personnel system etc>
- Maintains equipment to ensure Health and Safety is followed;
  <LIST e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers>
- Has separate curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  <LIST e.g. teachers access report writing module; SEN coordinator - SEN data>;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  <LIST e.g. teachers access their area / a staff shared area for planning documentation
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  [e.g. technical support or SIMS Support through LA systems; Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child]
- Provides pupils and staff with access to content and resources through the approved Learning Platform
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

Policy Updated Jan 2019
To be reviewed Jan 2021