Lea Community Primary School

eSafety Policy

Contents

Appendix:
Acceptable use policy: Staff and Governors
Acceptable use policy: Adults in school
Acceptable use policy: Children

eSafety Policy 2016 – Lea Community Primary School

1. Introduction

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

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

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

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

2. Lea Community Primary school's vision for eSafety

Lea Community Primary School aims to be an innovative learning community bound by strong values and committed to excellence. The School aims to provide a diverse, balanced and relevant approach to the use of technology.

- Through a variety of media the children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The school aims to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly.
- The school aims to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
- The users in the school community understand why there is a need for an eSafety Policy.

3. The role of the school's Senior Leadership Team

The roles of Lea Community Primary School's Senior Leadership Team include:

- having responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored. Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- 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. Policies and practices

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

- Behaviour Policy
- Acceptable use policy
- Anti-bullying policy
- ICT/Computing policy
- Teaching and learning policy
- Data protection policy

4.1 Security and data management

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

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- All laptops are password protected
- All children have their own password and are encouraged not to share it.
- All data in the school is kept secure and staff informed of what they can or can't do with data through the eSafety Policy, data protection policy and statements in the Acceptable Use Policy (AUP).
- The Senior Leadership Team are responsible for managing information
- Staff are aware of where data is located.
- All staff with access to personal data understand their responsibilities.
- The school ensures that data is appropriately managed both within and outside the school environment.
- The staff are aware that they should only use approved means to access, store and dispose of confidential data
- Staff have access to school logins, to ensure the data remains secure.
- The school's policy on using mobile devices and removable media is that school information is not allowed to be carried on pen drives and no school data is allowed to be removed out of school on removable devices.
- The school aims to ensure that data loss is managed by the use of passwords for the required people.
- The school's procedure for backing up data is remotely in a system which is managed by OneConnect.

.4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content.

Mobile phones are not encouraged to be brought into school by children. If a phone is brought in by mistake or is needed after school the children are asked to hand the phone in to a teacher or taken to the office.

4.3 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 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.
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs for personal use only – not to be used on social media sites
- 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. The 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 are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks. At all times staff are to be vigilant about use of communication technologies by the children and other staff members. This will be monitored closely alongside the Safeguarding Policy and Prevent Duty, as advised by the government.

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 Lea School's technical support (Blue Orange).
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

Lea Community Primary School email disclaimer:
****
This e-mail is confidential and privileged. If you are not the intended
recipient do not disclose, copy or distribute information in this e-mail
or take any action in reliance on its content.
****
This email has been checked for known viruses.

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

Mobile telephone use:

- Any staff and visitors who have mobile phones should turn them off during lesson time in school
- No photographs should be taken on a mobile phone except in extreme circumstances with approval from a member of the leadership team.
- Mobile phones may be used by staff members on trips to communicate with the school.

Web sites and other online publications

- 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 on the website.
- Everybody in the school aware of the guidance regarding personal information on the website.
- Teachers have access to edit the school website.
- The Head teacher has overall responsibility for what appears on the website.

4.5 Acceptable Use Policy (AUP)

Our Acceptable Use Policy is 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.

4.6 Dealing with incidents

Any incidents should be reported to the SLT as soon as possible.

- Minor incidents will be recorded in a log by the SLT. The eSafety coordinator will audit this log regularly.
- Any serious incidents or incidents involving illegal material will be referred to external agencies (e.g. the police, CEOP etc).

5. 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 default) by the Lancashire Grid for Learning. The School has devolved filtering to allow access to specific websites. Any websites which need to be ‘unblocked’ for an individual lesson should be reset on the same day.

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.

• All users of the school network have a secure username and password.

• The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in a secure place.
• Staff and pupils are reminded of the importance of keeping passwords secure
• Passwords will only be changed if the need arises.

Software/hardware
• The school has legal ownership of all software.
• The school has an up to date record of appropriate licences for all software and the ICT coordinator is responsible for maintaining this.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT 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 (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the SLT
- 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 your schools requirements / standards regarding eSafety
- The SLT is responsible for liaising with/managing the technical support staff.

6. Education and Training

6.1 eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. The school provides suitable eSafety education to all pupils:

- Regular, planned eSafety teaching within a range of curriculum areas.
- E-Safety education is differentiated for pupils with special educational needs.
- 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.
- Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules (See Appendices), acceptance of site policies when logging onto the school network.

6.2 eSafety – Staff training

- 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.
- Regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

6.3 eSafety – parents and carers

"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, homework diaries, Website,eSafety days.
- Promotion of external eSafety resources/online materials.

6.4 eSafety – Governors

The eSafety Policy will be reviewed yearly (and/or if a serious breach occurs) by the eSafety coordinator, approved by the governing body and made available on the school's website.

7 Standards and inspection

At Lea Community Primary School:

- E-Safety incidents are monitored, recorded and reviewed.
- The SLT are 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.

Developing and Reviewing this Policy

Policy Reviewed and adopted: February 2016
Next Review Date: February 2017

Acceptable Use Policy
Staff & Governors

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

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of Headteacher/Computing Coordinator.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. 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.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. 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.
19. 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 children to be safe and responsible in their use of ICT and related technologies.
20. 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 ……….

Supply teachers, students and other adults

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school’s network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children 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.
6. I will abide by the school’s rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. 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 ……….

Pupils

These rules reflect the content of our school's eSafety Policy. It is essential 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 not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
✓ I will only use the Internet and/or online tools when a trusted adult is present.
✓ I will only use my class e-mail address or my own school email address when emailing.
✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
✓ I will not deliberately bring in inappropriate electronic materials from home.
✓ I will not deliberately look for, or access inappropriate websites.
✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
✓ I will only communicate online with people a trusted adult has approved.
✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
✓ I will not tell other people my ICT passwords.
✓ I will not arrange to meet anyone that I have met online.
✓ I will only open/delete my own files.
✓ I will not attempt to download or install anything on to the school network without permission.
✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

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

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

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

This acceptable use policy must be signed and returned before any access to school systems is allowed.