Online Safety Policy
(Incorporating E-Safety, Responsible Internet Use & Safeguarding)

Please note that this is a summary document. For further details, please refer to the other policies referenced below.

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users). Our policy is based on the eSafety Guidance document provided by Lancashire Schools' ICT Centre. 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

Related school documents

- Behaviour Policy
- Anti-Bullying Policy
- Lancashire County Council ICT Security Framework for Schools
- Child Protection & Safeguarding Policy
- Acceptable Use Policy

Vision

Farington School recognises that ICT (Information and Communication Technology) is an important resource to support learning and teaching, as well as playing a significant role in the everyday lives of children, young people and adults. It is necessary that we build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. Farington Primary School aims to provide a diverse, balanced and relevant approach to the use of technology that gives our pupils both the skills and wisdom to use it both safely and effectively.

We aim to:

- Through a variety of media encourage the children to maximise the benefits and opportunities that technology has to offer.
- Ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- Equip our pupils with the skills and knowledge to use technology appropriately and responsibly.

- Recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- Ensure the users in the school community understand why there is a need for an eSafety Policy.

The role of the eSafety 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.
- Logging incidents as they occur and making changes where appropriate to improve safety.
- 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 Leader to ensure a co-ordinated approach across relevant safeguarding areas.

At Farington Primary School the eSafety Co-ordinator is the Headteacher.

Policies and Practice

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 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 permitted to be carried on pen drives encrypted pen drives outside of school, but only for the purpose of school related work. Data should then be returned to the secure school network, where it is also backed up.
- 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 to use the internal server and LCC's remote back-up solution for office data.

Use of mobile devices

Mobile phones are not encouraged to be brought into school by children. Should parents feel their child has a need to bring a phone into school they need explain that need to school staff. If a phone is brought in by mistake or is needed after school it is stored in the school office.

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

- 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 on entry to school but 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 if appropriate (the taking of photographs and/or videos are sometimes not permitted where parents would cause inconvenience or disruption by doing so.)
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of school and 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 not permitted to store digital content on personal equipment. Where there is a specific need to (e.g. an emergency / equipment failure etc), the digital content must be transferred to the network at the earliest opportunity and then deleted.
- 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 of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without 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 SLT and Governors.

Communication Technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.

- Only official email addresses are used for school matters between staff and parents regardless of whether when personal/sensitive data is involved. As a primary school, staff should not be communicating with children via e-mail.
- The Lancashire Grid for Learning filtering service reduces the amount of spam (Junk Mail) received on school email accounts. Any significant incidents of spam should be reported to the BT Lancashire Services
- 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).

Farington 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, 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 never be added as 'friends' on any Social Network site.
- Children who are under 13 are not legally allowed to be 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 must be assumed that 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.
- Mobile phones are not encouraged to be brought into school by children. Should parents feel their child has a need to bring a phone into school they need explain that need to school staff. If a phone is brought in by mistake or is needed after school it is stored in the school office.

Instant Messaging

Instant Messaging, e.g. MSN, Skype, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' these sites by default, but access permissions can be changed at the request of the Headteacher (See Appendix 1).

- Farington Primary School will ensure that Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.
- By way of helping children understand the appropriate use of messaging systems, Farington Primary School may on occasion use the secure messaging, forum or chat systems within their VLE (e.g.Moodle).

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 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 Headteacher has overall responsibility for what appears on the website.

Video conferencing

Video conferencing is not currently used at Farington Primary School.

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.

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 Pastoral 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.

Dealing with incidents

The SLT is responsible for dealing with eSafety incidents.

- Staff are aware of the different types of eSafety incident (illegal and inappropriate) and how to respond appropriately.
- Children are informed of relevant procedures through discussions with members of staff.
- Incidents are logged in a log book kept in the Headteacher's office.
- The above mentioned eSafety Incident Log is monitored on a regular basis and reviewed by the Governing Body Health & Safety Committee.
- The SLT will decide at which point parents or external agencies are involved

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). Staff should never personally investigate, interfere with or share evidence as they 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. They are licensed to investigate - schools are not! (See Appendix 11).

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.

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.

Accidental access to inappropriate materials

- Minimise the webpage/ Turn the monitor off/ click the 'Hector Protector' button.
- 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 / Deliberate searching for inappropriate materials / Bringing inappropriate electronic files from home / Using chats and forums in an inappropriate way.

- Inform SLT or designated eSafety co- ordinator.
- 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.

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.

Pupil access

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

Passwords

- Staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools.
- 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 Technician is responsible for maintaining this.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The Headteacher 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. 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 the ICT Technician.

Filtering and virus protection

Farington Primary School uses the LCC filtering system for school and regularly updates it's virus software.

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:

eSafety across the curriculum

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

- Regular, planned eSafety teaching within a range of curriculum areas (using the Lancashire ICT Progression framework).
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyber-bullying and how to seek help if they are affected by these issues.
- 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 / Moodle.

eSafety - Raising staff awareness

- All staff are regularly updated on their responsibilities
- 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/Acceptable Use Policy.
- Regular updates on curriculum resources and general eSafety issues are discussed in staff/team meetings.

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, homework diaries, Website, VLE/Moodle and other publications.
- Promotion of external eSafety resources/online materials.

eSafety - Raising Governors' awareness

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

Standards and inspection

At Farington 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 and these assessments are included in the appropriate policies as appropriate.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.