

Primary E-Safety Framework Document

Withnell Fold Primary School



E-Safety Policy 2024

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users). It is to safeguard and protect the children and staff, assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice and set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

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 E-Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our E-Safety 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.

This policy applies to all members of Withnell Fold Primary School and the community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. It sets out expectations for all school and community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).

2. Our school's vision for E-Safety

The E-Safety Policy is part of the Computing Policy and relates to other policies including those for behaviour, Safeguarding and RSHE. Reference to 'Internet Safety' is made in the scheme of work for RSHE.

Our E-Safety Policy has been written by the school, building on the LGfL policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We recognise that online safety and broader digital resilience must be thread throughout the curriculum.

How does the Internet benefit education?

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the DfES ICT in Schools;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and DfES.
- mentoring of pupils and provide peer support for them and teachers

How will Internet use enhance learning?

- The school Internet access is designed expressly for pupil and staff use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Use of the Internet will be built into curriculum planning to specifically enrich and extend the learning process not only in school but at home. It will support remote learning and the delivery of homework.
Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. The role of the school's eSafety Champion

Our E-Safety Champion is Mrs Moreton

The role of the E-Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's E-Safety Policy and associated documents.
- 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 E-Safety incident occur.
- Ensuring the E-Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with E-Safety 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 E-Safety advice/training for staff, parents/carers and governors.

4. Policies and practices

E-safety is taken seriously at Withnell Fold. Any breaches of policy must be reported directly to the Head Teacher for investigation.

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

Anti-bullying
Safeguarding
Behaviour

4.1 Security and data management

In line with the requirements of the Data Protection Act 2018 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.

The Head Teacher has overall responsibility for the management of data within school.

Sensitive data is only stored on the office system. The users of this system are: the Head Teacher and School Bursar. These staff members are aware of their legal responsibilities. There is no access to this information from the curriculum system.

Confidential data must only be accessed with approval from the Head Teacher. Paper copies must be stored in the office (not classrooms) and must be shredded on site for disposal. Any data should be kept confidential and treated with sensitivity.

Any data loss MUST BE reported to the Head Teacher or E-Safety champion immediately.

The school provides staff with individual log-ins; all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private. The pupils are provided with safe pupil log-ins as part of their class. The network is set up 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. Staff and pupils are encouraged to log off when they have finished working or are leaving their computer unattended.

4.2 Use of mobile devices

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

Teaching staff may use information stored on a hard drive providing they ensure that the content is age-appropriate and that their hard drive is virus-checked before use on the school system (with a view to move over to the 'Cloud')

Pupils are not allowed to bring mobile phones into school except in rare circumstances and with the permission of the Head Teacher, without this permission mobile devices will be confiscated and returned to an appropriate adult. On the rare occasion pupils may need to bring mobile phones into school, these must be handed to the headteacher until the end of the school day.

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. 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.

Copyright infringement - Copyright law applies on the internet but is ignored by many who download and swap files and copy and paste text and graphics. Staff need to be aware of copyright laws linked to pictures and videos they are using and cite these as appropriate.

As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (2018), we ensure we have written permission for their use from the individual and/or their parents or carers. This information is collected when a child starts school and an up-to-date list is obtainable from the office. The permission is made in terms of the intended use of the photograph. No names will be attached to photographs on the website or in the local media without the permission of the person involved and no children's names will be attached to photographs on the school website.

Photographs and videos must only be taken on school equipment and must not be taken off the school premises.

- Parents/carers, who have been invited to attend school events, are allowed to take photographs. They should be made aware that these must only be for personal use in advance.
- Training has taken place to ensure that staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- When taking photographs/video, staff must ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved is an offence.

These guidelines are monitored annually by the E-Safety champion.

4.4 Communication technologies

Email:

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

- All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
- Only official email addresses should be used to contact staff/pupils.
- Staff have school closure emails that were set during COVID remote learning and these should be used by parents to communicate with staff in the event of a school closure.
- The Lancashire Grid for Learning filtering service plus (Clutter) should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to One Connect.
- 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 (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

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

GUIDANCE AND ADVICE

Employees who choose to make use of social networking site/media should be advised as follows: -

- That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended.
- That they do not conduct or portray themselves in a manner which may:-
 - bring the school into disrepute;
 - lead to valid parental complaints;
 - be deemed as derogatory towards the school and/or its employees;
 - be deemed as derogatory towards pupils and/or parents and carers;
 - bring into question their appropriateness to work with children and young people.
- That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.
- On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

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.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile phones:

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

Pupils are not allowed to use mobile phones in school.

Staff phones must be turned to silent during teaching sessions.

Visitors may use mobile phones outside the classroom.

Personal mobile phones may be used on school visits but personal phone numbers must not be used on any documents which parents or pupils may have access to.

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of 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 Head Teacher.

Web sites and other online publications

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

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Downloadable materials must be in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

X

X is a social media tool that currently has no age restrictions for its use. X is used to communicate thoughts and ideas within 280 characters and usually references people, places and activities that tend to invite replies. X user accounts can follow other X User accounts or be followed by other X user accounts and all tweets are public. Users are able to Direct Message (DM) other users should they wish something not to be made for public viewing.

Only the SLT will have access to the official school twitter account. As the school moves forward with X, other staff members may be invited to tweet from the official school account. Should this happen, this policy will be updated.

X will not be used to engage with individual parents directly, however, important announcements and notices could be sent as part of general communication to parents, to advertise and promote the school, to encourage people to visit the school blog and to show off the wonderful things happening at Withnell Fold.

Video conferencing:

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

- A permissions letter must be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children will not be appearing 'live' on the Internet through a video conferencing link aside from school celebration assemblies via zoom and zoom sessions if the school should have to be in contact with students during a period of remote learning. There is a separate policy for the use of Zoom.
- However, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.
- Approval by the Head Teacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

4.5 Dealing with incidents

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LCC can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. The Head Teacher will ensure that the Internet policy is implemented and compliance with the policy monitored. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head Teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate,

interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation. (<http://www.iwf.org.uk>). They are licensed to investigate – schools are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website

Inappropriate Use

Incident	Response
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 Champion. Enter the details in the Incident Log. Additional awareness raising of eSafety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carers involvement

5. Infrastructure and technology

Pupil Access:

Pupils will only have supervised access to the internet. No access will be allowed during unsupervised times such as playtime or lunchtime. Pupils will only be allowed access when a positive consent form has been returned. An up-to-date list is available from the school office.

Passwords:

Children only have class access. Teachers have class and staff access. The administrator password is only known by the ICT technician and the Computing Coordinator.

Software/hardware:

School has legal ownership of all software, including site licences where appropriate.

Licenses for all software are kept in a secure place by the Computing subject leader.

The Computing subject leader regularly audits equipment and software.

Control over what software is installed on school systems is maintained by the Computing subject leader.

Should a child require a device for remote learning they must sign the home/school agreement which sets out the expectations of using the device at home.

Managing the network and technical support:

The network is managed and technical support provided by BTLS.

- LGfL/CLEO Servers are located in a secure cupboard where there is no pupil access.
- All wireless devices have had their security enabled.

- The technician is responsible for managing the security of the curriculum school network.
- Computers are regularly updated with critical software updates/patches by the technician.
- Breaches of security must be reported immediately to the Head Teacher or the Computing subject leader.
- Laptops may be used for personal use but must not be used by family members.
- Technical support providers are made aware of our schools requirements/standards regarding eSafety.
- It is the Computing subject leader's responsibility to liaise with/manage the technical support staff.

Filtering and virus protection:

- The School has educational filtered secure broadband and can be personalised and managed by the school. The filtering system blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status. Filtering may be performed by the ISP, by the LEA, at school-level or by any combination.
- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing subject leader.
- Staff are expected to bring their laptops into school on a regular basis to have security software updated.
- Suspected or actual computer virus infection should be reported immediately to the ICT subject leader or technician.

6. Education and Training

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

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

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus', Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact Sexting Upskirting

6.1 eSafety across the curriculum

- The Lancashire ICT progression document is used as a starting point for eSafety awareness training for pupils.
- Pupils will be taught be SMART; to STOP and THINK before they CLICK and acknowledge the source of information used. They will be taught to respect copyright when using Internet material in their own work.

- Pupils in Key stage 2 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 or worry boxes.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Rules for Internet access will be posted in all classrooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Children will be taught how to report any abuse including bullying; how to seek help if they experience problems when using the internet and related technologies. A module on responsible Internet use is included in the PSHE programme covering both school and home use and as part of Digital Literacy in the Computing programme.

Pupils are taught to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

6.2 E-Safety – Raising staff awareness

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
 - All staff including teachers, supply staff, classroom assistants and support staff, will be provided with ICT Acceptable use Policy, and its importance explained.
 - Staff should be aware that Internet traffic can be monitored and traced to the individual user. Staff will know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity required data protection.
- Discretion and professional conduct is essential.
- Regular training will be organised by the eSafety champion for all staff.

6.3 E-Safety – 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).

- Further information for parents is available on the school website.
- Information on eSafety is included in newsletters to parents when appropriate, along with the Promotion of external eSafety resources/online materials.

Parents should know and understand what the 'the rules of appropriate use' are and ensure they have signed the Acceptable Use Policy.

6.4 E-Safety – Raising Governors' awareness

The E-Safety Policy should be regularly reviewed and approved by the governing body.

7. Standards and inspection

- The E-Safety policy will be reviewed annually and will incorporate new technologies.
- A risk assessment will be carried out before any new technology is incorporated into teaching and learning. These risk assessments will be incorporated into the policy.

- ESafety incidents will be monitored and recorded by the Head Teacher. These will be analysed to see if there is a recurring pattern.
- Patterns of eSafety issues will be addressed thorough assemblies, workshops and 'Circle Time' activities where appropriate.
- Changes to the eSafety policy will be discussed at staff meetings and staff will disseminate this information to pupils in an age-appropriate way.
- The eSafety policy will be reviewed by the curriculum sub-committee of the governing body and will be made available to parents.
- AUPs will be reviewed annually in the light of emerging technologies.

Reviewed – September 2024

Next review – September 2026