**Online Safety Policy**

Spring 2025

**Summary**

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-bullying, Child Protection, Curriculum, Data Protection, Staff Handbook and Safe Working Practice Policy.

A copy will be made available to parents/carers, staff, governors and representatives of partner agencies through our school website and upon request.

|  |  |
| --- | --- |
| Author’s Role | Computing Lead |
| Date | Spring 2025 |
| Internal Review date | Spring 2026 |
| Review date | As changes |

**Teaching and learning**

**Why the Internet and digital communications are important:**

* The Internet is an essential element in 21st century life for education, business and social interaction.
* The school has a duty to provide pupils with quality Internet access as part of their learning experience.
* Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
* Many pupils will use the internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

**Internet use will enhance learning**

* The school Internet access will be designed expressly for pupil 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.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
* Pupils will be shown how to publish and present information to a wider audience.

**Pupils will be taught how to evaluate Internet content**

* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
* Pupils will be taught the importance of cross-checking information before accepting its accuracy.
* Pupils will be taught how to report unpleasant Internet content

**Managing Internet Access**

**Information system security**

* School IT systems security will be reviewed regularly.
* Virus protection will be updated regularly.
* Security strategies will be discussed with the Local Authority.

**E-mail**

* Pupils may only use approved e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail.
* In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
* Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
* The school should consider how e-mail from pupils to external bodies is presented and controlled.
* The forwarding of chain letters is not permitted.

**Published content and the school website**

* Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
* The Computing lead will ensure that content is accurate and appropriate.
* The management and build of the website is via a third party.

**Publishing pupil’s images and work**

* Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
* Pupils full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.
* Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
* Work can only be published with the permission of the pupil and parents/carers.
* Pupil image file names will not refer to the pupil by name.
* Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

**Social networking and personal publishing**

* The school will control access to social networking sites, and consider how to educate pupils in their safe use.
* Newsgroups will be blocked unless a specific use is approved.
* Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
* Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
* Pupils will be advised to use nicknames and avatars when using social networking sites.

**Managing filtering**

* The school will work with Data Cable over any issues regarding filtering of content.
* If staff or pupils come across unsuitable on-line materials, the site must be reported to the online safety Coordinator who will then check the content and then request the site be blocked through the on-line blocking facility.

**Managing videoconferencing & webcam use**

* Videoconferencing should use the educational broadband network to ensure quality of service and security.
* Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
* Videoconferencing and webcam use will be appropriately supervised for the pupils age.

**Managing emerging technologies**

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
* The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lessons or formal school time.
* The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
* The use by pupils of cameras in mobile phones will be kept under review.

**Protecting personal data**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
* Refer to the Data Protection Policy.

**Policy Decisions**

**Authorising Internet access**

* All staff must read and sign the *Staff, Governor and Visitor Acceptable Use Agreement* before using any school IT resource.
* The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
* At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
* Parents will be asked to sign and return a consent form.
* Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

**Assessing risks**

* The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network.
* The school will audit IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

**Handling online safety complaints**

* Complaints of Internet misuse will be dealt with by a senior member of staff.
* Any complaint about staff misuse must be referred to the Head teacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Pupils and parents will be informed of the complaints procedure (see schools complaints policy) Pupils and parents will be informed of consequences for pupils misusing the Internet.

**Communications Policy**

**Introducing the online safety policy to pupils**

* Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
* Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
* Online safety training will be embedded within the Computing scheme of work or the Personal Social and Health Economic (PSHE) curriculum.
* Staff will use the ProjectEVOLVE toolkit is based on the UKCIS framework “Education for a Connected World” (EFACW). This framework covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes or competencies are mapped to age and progress. The statements guide educators to the areas that they should be discussing with children as they develop their use of online technology.

**Staff and the online safety policy**

* All staff will be given the school online safety policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
* Staff will always use a child friendly safe search engine when accessing the web with pupils.

**Enlisting parents’ and carers’ support**

* Parents and carers attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
* Monthly Online safety newsletters are shared with parents and available on the school website
* The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

**Appendix A -** Flow Chart for responding to online safety incidents

**Appendix B -** Acceptable ICT Use Agreement: KS2 pupils and parents

**Appendix C -** Acceptable ICT Use Agreement: KS1 pupils and parents

**Appendix D-** Acceptable ICT Use Agreement: Staff, Governor and Visitor

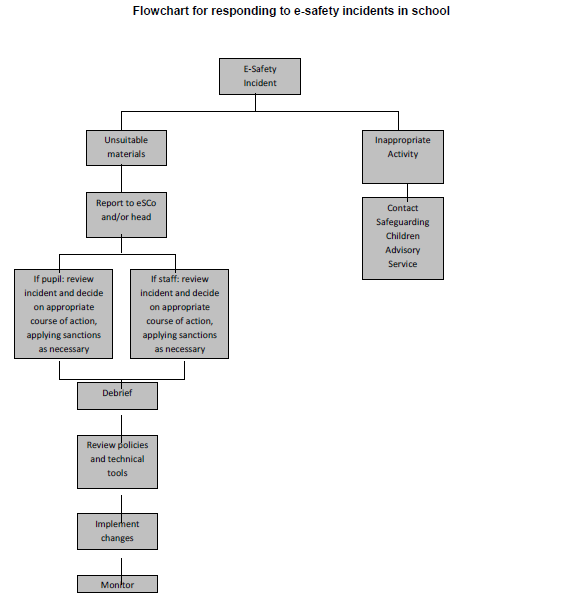
**Appendix E** – EYFS Policy for the use of mobile phones and cameras

**Appendix F** – Protocol for the use of mobile phones

**Appendix G** – Mobile phone security protection

**Appendix H** – Ipad acceptable Use Agreement : Staff

**APPENDIX A – Flowchart for responding to online safety incidents** this was from a previous safeguarding doc, there will be something more up to date available

****

**APPENDIX B – Internet letter and Acceptable Use Agreement KS2**

Responsible use of the internet

As part of our ICT provision at Fieldhead Carr we encourage all children to behave appropriately and use equipment with care. That means making sure children make choices that keep them safe.

Attached to this letter is an Acceptable Use Policy. This has been discussed in class and I would like you to talk to your child about it. You will both need to sign and return to school.

All KS2 children receive a school email account, this is a secure account provided by Microsoft360. Staff in Y3 teach children how to use email and share online safety guidelines through the computing curriculum.

Please read, sign and return the Acceptable Use Policy by

Yours sincerely,

Mrs L Warner

Computing Leader

 **Fieldhead Carr Primary School**

**KS2 Pupil Acceptable Use Agreement**

* I will only use ICT in school for school purposes.
* I will only use my own school email address when emailing.
* I will only open email attachments from people I know, or that my teacher has approved
* I will not tell other people my passwords for the school network, or other learning websites
* I will only open/delete my own files
* I will make sure that all ICT related contact with other children and adults is appropriate and polite
* I will not deliberately look for, save or send anything that could offend others
* If I accidently find anything inappropriate on the internet I will tell my teacher immediately
* I will not give out my personal details such as my full name, phone number, home address or school
* I will be responsible for my behaviour when using ICT in school or at home because I know these rules are to keep me safe.
* I know that my use of ICT can be checked and that my parent or carer contacted if a member of school staff if concerned about my safety.

Pupil signature .........................................................................

Print name ..............................................................................

Parent signature .....................................................................

Print name ..............................................................................

Date ........................................................................................

**APPENDIX C – Acceptable Use Agreement KS1**

Fieldhead Carr Primary School

### E

## **If I see something I don’t like on a screen, I will always tell an adult.**

### F

I will only send friendly and polite messages.

### A

# I will only access my own work. I will only click on icons and links when I know they are safe

### S

# I will only use the Internet when an adult is there.

KS1 Acceptable Use Policy

## **Think before you click!**

My Name:

My Signature:

Parent/Carer:

Date:

**APPENDIX D – Acceptable Use Agreement**

**Fieldhead Carr Primary School**

**Staff, Governor and Visitor Acceptable Use Agreement**

**IT and the related technologies such as email, the internet and mobile devises are an expected part of our daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of IT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy conforming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with Lisa Warner (Computing Leader)**

**Members of staff should consult the school’s e-safety policy for further information and clarification.**

* I understand that it is a breach of policy to use a school IT system for a purpose not permitted by its owner. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
* I will only use the school’s email/internet/Learning Platform and any related technologies for professional purposes or for uses deemed “reasonable” by the Head teacher or Governing Body.
* I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
* I will not install any software or hardware without permission.
* I will report any accidental access to inappropriate materials immediately to my line manager
* I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
* I will respect copyright and intellectual property rights.
* I will report any incidents of concern regarding children’s safety to the Designated Child Protection Coordinator or Head teacher.
* Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher in line with data security policy.
* I will ensure that electronic communications with pupils including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
* I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
* I will support and promote e-safety and will help pupils to be safe and responsible in their use of IT systems, communications and publishing.
* The school may exercise its right to monitor the use of the school’s information systems, Internet access, and e-mail and to delete inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
* **I agree to follow this acceptable use policy and to support the safe use of IT throughout the school**

Signed: ………………………………............... Print: …………………………………….......... Date: …………….……

**APPENDIX E – EYFS Mobile phone and camera Policy**

 EARLY YEARS FOUNDATION STAGE POLICY FOR THE USE OF CAMERAS AND MOBILE PHONES

To ensure the safety and welfare of the children in our care this policy outlines the protocols for the use of personal mobile phones and cameras in the setting.

* Personal mobile phones, cameras and video recorders cannot be used when in the presence of children either on school premises or when on outings.
* All mobile phones must be stored securely within the setting during contact time with children. (This includes staff, visitors, parents, volunteers and students).
* No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings. School policy regarding this matter should be explained clearly to Parents by the EYFS Leader.
* Mobile phones must not be used in any teaching area within the setting or within the bathroom area.
* In the case of a personal emergency staff should use the school telephone. It is the responsibility of all staff to make families aware of the school telephone numbers.
* Personal calls may be made in non-contact time but not within the teaching areas.
* Personal mobiles, cameras or video recorders should not be used to record classroom activities. ONLY school equipment should be used.
* Photographs and recordings can only be transferred to and stored on a school computer before printing.
* All telephone contact with Parents/Carers must be made on the school telephone.
* During group outings nominated staff will have access to the school mobile which can be used in an emergency or for contact purposes.
* In the case of school productions, Parents/carers are permitted to take photographs of their own child in accordance with school protocols which strongly advise against the publication of any such photographs on Social networking sites.

MONITORING AND REVIEW:

It is the responsibility of all staff to adhere to this policy. It will be reviewed annually by the Governing body.

February 2024

**APPENDIX F – Protocol for the use of Mobile Phones**

**Fieldhead Carr Primary School**

**Protocol for the use of Mobile Phones**

**Introduction**

The purpose of this protocol is to inform employees of the expectations of mobile phone use during their working hours. It is intended to give staff some broad guidelines regarding appropriate use of mobile phones, in the workplace or in the course of carrying out your duties.

This protocol will operate in conjunction with other policies including those for Child Protection, Staff Handbook, Safe Working Practise, Data Protection and Security.

**Use of mobile phones during the working day**

The use of mobile phones by employees to make/receive personal calls and/or texts during the working day is discouraged for the following reasons (this list is not exhaustive)

* It does not set a professional and positive example to pupils, it is disruptive and interrupts lessons
* It is a nuisance/discourteous to colleagues (eg during meetings)
* It is a misuse of the school/authority’s time and has the potential to impact on children’s learning

Mobile phones should be stored securely within the setting during contact time with children. Mobile phones must not be used in any teaching area.

Any personal calls should be directed to the school’s landline number so that a message can be relayed to the member of staff, when the member of staff is available, unless there is an emergency situation, where the message must be relayed to the employee immediately.

Employees using mobile phones during breaks should be respectful of their colleagues and mobile phones should not be used in front of pupils.

An increasing number of mobile phones now have built in cameras and have the capability to capture, copy and transmit images through a range of technologies and formats. Employees should not take or transmit images of pupils and colleagues on their personal mobile phone.

**Business use**

Any employees, who have been provided with a mobile phone for business use, must ensure the mobile used is solely for this reason, unless express permission has been given that the phone can also be used for personal use.

**Security**

Employees accessing emails using either their personal or business phones should have the appropriate secure systems in place to ensure should their phone be lost or stolen, the data cannot be accessed.

Employees should be requested to sign a declaration to ensure their phone is password or pin protected. This should be signed and kept on the employee’s personal file.

**Social Networking**

Employees should not access social networking sites via their mobile phones (business or personal phones) during working hours.

**Protection of Employees**

Employees should not provide parents or pupils with their personal mobile phone number.

Employees should refer to the School’s Protocol for the use of texting/phoning parents where one exists.

**Mobile phones and pupils**

School has a separate policy which covers the use of mobile phones by pupils.

Employees should be aware that there may be occasions where pupils could provoke staff to gain a particular reaction which may then be recorded.

If an employee receives material deemed to be inappropriate or offensive, the images/text should be retained as evidence and referred immediately to the headteacher/designated Manager.

**Appendix G – Mobile phone is securely protected for purposes of accessing Microsoft360**

I can confirm that my mobile phone is securely protected for the purposes of accessing my School email and sharepoint account. The security is in the form of

…………………………………………………………………………………………… (eg password or encryption)

Signed ………………………………………………

Dated………………………………………………..

**APPENDIX H – ipad Acceptable Use Agreement for Staff**

**Fieldhead Carr Primary School iPad Acceptable Use Agreement(Adults)**

The policies, procedures and information within this document applies to all iPads, iPods Touches or other IT handheld devices used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

**User responsibilities**

* The user must use protective covers/cases for their iPad.
* The iPad screen is made of glass and therefore subject to cracking and breaking if misused: Never drop nor place heavy objects (books. Laptops, etc) on top of the iPad.
* Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
* Do not subject the iPad to extreme heat or cold.
* Do not store or leave unattended in vehicles.
* Users in breach of the Acceptable Use Agreement may be subject to but not limited to: disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
* Memory space is limited. Academic content takes precedence over personal files and apps.
* The whereabouts of the iPad should be known at all times.
* It is the user’s responsibility to keep their iPad safe and secure at all times.
* If an iPad is found unattended, it should be given to the nearest member of staff.

**Lost, Damaged or Stolen iPad**

* If the iPad is lost, stolen or damaged, the Head teacher must be notified immediately
* iPads that are believed to be stolen can be tracked through the icloud

**Prohibited Uses (not exclusive)**

* Accessing inappropriate materials – All material on the iPad must adhere to the Acceptable Use Agreement
* Cameras – Users must adhere to the Policies: Staff Handbook, Safe Working Practise Policy, EYFS policy on Mobile phones and cameras, along with Protocol for the use of mobile phones.
* Any users caught trying to gain access to another’s user accounts, files or data will be subject to disciplinary action.
* Jailbreaking – Jailbreaking is the process of which removes any limitations place on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
* Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action
* Misuse of passwords, Codes of other Unauthorised Access: Users are encouraged to set a pass code on their iPad to prevent other users from misusing it.
* Users should be aware of and abide by the guidelines set by the school’s online safety policy.
* Fieldhead Carr reserves to the right to confiscate and search and iPad to ensure compatibility with this Responsible Use Agreement
* Adult users must read and sign below

I have read, understand and agree to abide by the terms of the iPad Responsible Use Policy.

I can confirm that the iPad is securely protected.

The security is in the form of

……………………………………………………………………………… (eg password or encryption)

Signed ………………………………………………

Date………………………………………………..