Policy for E-Safety

Introduction

This document was reviewed during the Autumn term 2025
This policy will be reviewed in the Autumn term 2026

School Aims

We want our children to **believe** in themselves, **achieve** and **succeed**.
Our aims are

- To ensure all children have access to a broad, balanced and engaging national and locally relevant curriculum that fosters high expectations for all pupils.
- To provide a caring, secure and supportive environment where children can develop respect and belief in themselves, others and their surroundings and feel confident to express their individuality.
- To promote and inspire curiosity, resilience and independence within the children
- To value our community, the richness of other cultures and the world we live in
- To understand and promote the importance of being active and healthy

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The school's e-safety Policy will operate in conjunction with other policies including those for behaviour, anti-bullying, curriculum, data protection, safeguarding and security.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure network design and use.
- Safe and secure broadband provided by Northumberland Network

School e-safety policy

The e-safety policy is part of the school development plan and relates to other policies including those for ICT, bullying and child protection.

- The school will appoint an e-safety coordinator – Mrs Currans (not a technical role). She is a safeguarding lead as the roles overlap.

- Our e-safety policy has been written by the school, building on the Kent e-safety policy and government guidance. It has been agreed by senior management and approved by governors and Northumberland ICT team.
- The e-safety policy and its implementation will be reviewed bi-annually.
- The e-safety policy will be revised by: the Computing subject lead and one of the safeguarding leads.

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils

Internet will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly
- Lightspeed to access internet by anyone on computers available to children (username and password required)
- PCE is installed on all computers and laptops including teachers' laptops
- PCE data will be monitored by ICT co-ordinators

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.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission

Published content and the school website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published

Publishing pupil's images and work

- 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.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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 or their location.

Managing filtering

- The school will work with the LA to ensure systems to protect pupils are reviewed and improved.
- Weekly checks from PCE reports
- If staff or pupils discover an unsuitable site it must be reported to the ICT coordinators.

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.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy decisions

Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date.
- EYFS access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. In Year 1 and onwards all children will have their own username and password to access the internet which will be monitored for inappropriate use by PCE.
- Parents will be asked to sign and return a consent form.
- Pupils must read and sign (age permitting) an 'acceptable use of ICT agreement'

Assessing risks

- 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 NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school protection procedures.
- The school will follow the complaint procedure as recommended by NCC

Communications policy

Introducing the e-safety policy to pupils
- E-safety rules will be displayed in classrooms and discussed with pupils.
- Pupils will be taught about e-safety at an age appropriate level.

Staff and the e-Safety policy
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support
- Parents' attention will be drawn to the School e-Safety Policy on the school website.

Pupils' use of internet

• Use of the internet, including e-mail, is permitted as directed by the teacher for purposes such as: - research and learning activities directly related to the curriculum.
• Pupils will only be able to download a file under the direct supervision of a member of staff and it will be virus checked prior to being opened.
• The use of game-style activities should be monitored by the teacher to determine suitability. Violent games are NOT permitted.
• Personal e-mail, social networking or instant messaging sites are NOT to be accessed by pupils.
• Children should report any misuse of the internet to their teacher.
• Children should be made aware of the possibility and consequences of online bullying.
• When e-mail is required as part of a curriculum based lesson, ALL e-mails transmitted and received will be approved by teaching staff.
• No emails will be approved where it may include information that may offend others or where it does not respect the rights, beliefs and feelings of others. Pupils of Prior Park First School should always remember that they are representing themselves and our school.

• Personal information such as full names, home addresses, and phone numbers will NEVER be sent by email.

Pupils are not permitted to bring mobile phones, any other electronic device or Smart watches to school.

Prior Park Primary School
Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offense to use the school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information services may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and will not disclose any password or security information to anyone other an authorised system manager.
- I will not install any hardware or software without permission.
- I will ensure that personal data is stored correctly and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils (email) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept 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 so for storing unauthorised or unlawful text, imagery or sound

.

I have read, understood and accept the Staff Code of Conduct for ICT

Signed:…….
Date:……..