Pegswood Primary School

E-Safety Policy
September 2025

Created by: <u>A Waterfield</u>   Date: <u>Sept 2025</u>

Approved by Governors:_____   Date:_____

Headteacher:_____   Date:__30-9-25__

Review Date: <u>Sept 2026</u>

PEGSWOOD PRIMARY SCHOOL

E-SAFETY POLICY

Our e-Safety Policy has been written by the school following government guidance and approved by Governing Body.

We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. There are many online safeguarding issues that can be categorised into four areas of risk:

Content:	Being exposed to illegal, inappropriate or harmful material such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact:	Being subjected to harmful online interaction with other users such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct:	Personal online behaviour that increases the likelihood of, or causes, harm such as making, sending and receiving explicit images.
Commerce:	Risk such as online gambling, inappropriate advertising, phishing and of financial scams

(Amended from 'Keeping Children Safe in Education')

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We work hard to increase parents' understanding of the internet and of the serious safeguarding issues and risks that there are for children online and how to keep them safe.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment, we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

<u>Teaching and Learning</u>

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 a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning
- The school's 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

<u>Managing Internet Access</u>

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Northumberland LA.

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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school-headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully to ensure they are appropriate.
- Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or other social media.
- Pupil's work can only be published with the permission of the pupil and parents.

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.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary-aged pupils.

Managing filtering

To block harmful/inappropriate content, we have a contract with Northumberland County Council to provide and manage our internet use, as well as Fortinet to provide a secure and filtered Internet service, which enables us to access and use the Internet and all email safely. The Internet filtering service will be annually reviewed. We recognise that not all filters are 100% accurate; therefore, we ensure we regularly teach the children online safety rules so they can assess and manage risk for themselves. Additionally, as a school, all of our devices have Senso, which is used to monitor activity. Weekly reports are sent to the headteacher and DSL.

Access to the Internet is designed to protect pupils and school personnel by blocking the following content:

- adult content containing sexually explicit images
- violent content containing graphically violent images
- hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- illegal drug taking content relating to the use or promotion of illegal drugs or the misuse of prescription drugs
- criminal content relating to the promotion of criminal and other activities
- gambling content relating to the use of online gambling websites
- non-educational websites such as social networking sites

All users access the Internet in accordance with the School's Acceptable Internet Use & Agreement and will inform the ICT coordinator if at any time they find they have accessed inappropriate Internet sites.

- When inappropriate material has been accessed, the Internet Service Provider will be contacted, and if necessary, the Police.

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.
- Mobile phones will not be allowed in school.
- Staff will use a school phone where contact with pupils is required.

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, for instance, a member of staff may leave or a pupil's access may be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional direct supervised access to specific, approved online materials.
- Parents will be asked to sign and return a consent form.

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 if its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the headteacher.
- 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 child protection procedures.

- Pupils and parents will be informed of the complaint procedure.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be discussed with the pupils at the start of each year.
- Pupils will be informed that Internet use will be monitored.

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 are essential.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters and through school communication.

Failure to Comply

- Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by the headteacher.

Version	Reason for Amendments/Update/Review	Date of Adoption	Date of next review
1.0	New policy	Sept 2024	Sept 2025
2.0	Learner agreement added	Sept 2025	Sept 2026

Appendix 1

Acceptable Use Agreement – Pupil

PUPIL ACCEPTABLE USE AGREEMENT / E-SAFETY RULES

Dear Parent/ Carer

ICT including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

- I will only use ICT in school for school purposes.
- I will only use my class email address.
- I will make sure that all ICT contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.
- I will not send to children or adults anything that could be considered
- unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home
- address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
  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 e-Safety.

Parent/ carer signature

We have discussed this and _____(child's name) agrees to

follow the e-Safety rules and to support the safe use of ICT at Pegswood Primary School.

Name   _____

Parent/ Carer Signature   _____

Date   _____

Appendix 2

Acceptable Use Agreement – Staff

STAFF ACCEPTABLE USE AGREEMENT / CODE OF CONDUCT

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher, School e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for use deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues' material that could be considered offensive or illegal
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout Pegswood Primary School.

Signature _____ Date _____

Full Name _____