Online Safety (E-Safety) Policy

Purpose

This policy sets out how Portavogie Primary School promotes safe, respectful and responsible online behaviour and responds to concerns. Online safety forms part of the school's safeguarding and preventative education arrangements. It applies to pupils, staff, governors, volunteers and school-provided digital systems, including off-site activity where school safeguarding responsibilities arise.

Core principles

Online safety education is as important as technical protection. Filtering and monitoring provide safeguards but cannot replace supervision, sound professional judgement or a culture in which children feel able to tell an adult about worries.

The school teaches children to protect personal information, treat others respectfully, think critically about online information, recognise harmful or suspicious contact and seek help. Materials and explanations will be age-appropriate and accessible.

Responsibilities

The Board of Governors provides oversight of policy and safeguarding arrangements. The Principal ensures procedures, training and oversight of reported concerns.

The Designated Teacher for Child Protection, Mrs Kim Spence, leads the safeguarding response to online concerns, supported by the relevant deputy/designated safeguarding staff in accordance with the school's Safeguarding and Child Protection Policy. Staff report concerns promptly to the Designated Teacher or appropriate deputy, not solely to the ICT Coordinator.

The ICT Coordinator, Miss Joanne Johnston, supports online safety education, staff awareness and liaison on technical matters, but does not replace designated safeguarding staff. All adults follow school policies, model safe use and respond promptly to pupil disclosures.

Access, supervision and account security

Pupils use age-appropriate school-approved resources with appropriate adult supervision. Staff check proposed websites and applications, consider privacy and safeguarding risks and use school-approved systems and accounts.

Staff and pupils must keep individual credentials private. Staff must not share passwords with colleagues or pupils; technical access and account resets follow authorised procedures. Multi-factor authentication is used where supported and required.

Unauthorised software, personal accounts for pupil communication and use of personal devices for storing pupil data are not permitted unless specifically approved under school

procedures. Suspected phishing, lost devices, breaches or inappropriate material must be reported promptly through the relevant school and technical channels.

Online safety education

Foundation Stage and Key Stage 1 pupils are taught simple rules: ask a trusted adult, use approved links, keep private information private, be kind and tell someone if anything feels wrong.

Key Stage 2 teaching develops understanding of privacy settings, contact from strangers, scams, cyberbullying, misinformation, manipulated and AI-generated media, online gaming, digital footprints and where to find help.

Parents and carers receive information or signposting to trusted sources including Safer Schools NI, CEOP/Thinkuknow and Childnet where appropriate.

Acceptable use and pupil devices

Pupils must use the internet and school digital equipment only for appropriate activities, with permission and suitable supervision. They must not deliberately search for harmful content, misuse school accounts, share passwords or photograph or record others without permission.

Pupils are not permitted to use personal mobile phones during the school day. Any exceptional arrangement, including a disability-related or other agreed need, must be authorised by the Principal and clearly communicated to the pupil and family. Staff will follow current DE guidance on mobile phones and the school's established rules on bringing and storing devices.

Breaches are handled fairly under the Positive Behaviour Policy and Addressing Bullying Policy, with consideration of a child's age, needs, context and any safeguarding concerns.

Reporting and responding to concerns

Any pupil who encounters upsetting material, unwanted contact or online bullying should tell a trusted adult. Staff listen calmly, record the facts and refer safeguarding concerns immediately using the school's safeguarding procedures. Do not promise confidentiality or investigate child protection matters independently.

Where harmful digital content or an image is involved, staff should not forward or unnecessarily copy it, particularly if it may contain an indecent image of a child. Preserve relevant information safely, follow the safeguarding response and seek appropriate specialist advice. Immediate risks are escalated promptly to the appropriate agencies.

Online bullying, including activity occurring outside school which affects school life, is addressed consistently with the school's Addressing Bullying Policy and relevant Northern Ireland requirements. Records are kept under established safeguarding, behaviour and data protection arrangements, not an unofficial ICT log.

Images, communication, AI and data

School photographs, videos and publications are governed by safeguarding checks, the school's photograph permissions and privacy arrangements, and the Social Media Policy. Staff use approved channels for communications with parents and pupils and maintain professional boundaries.

Staff must not input identifiable pupil information, confidential records or safeguarding material into public AI services without express school approval and a suitable data protection assessment. AI outputs should be checked for accuracy and appropriateness. No AI-manipulated pupil image or misleading representation may be published without appropriate review and authority.

For 2026/27, the school uses a Digital Images, Photographs and Video Consent Form with separate Yes/No choices for use within school, printed publications, the website, the official Facebook page, newspapers and recognised media, and trusted external organisations. Staff must check the relevant choice for each pupil before taking or using images for that purpose. A missing, blank or unclear response must not be treated as permission to publish. Safeguarding restrictions take priority even where permission has been given.

Parents and carers can change or withdraw their choices by contacting the school. The school keeps its permissions record up to date, communicates changes to relevant staff and removes school-controlled online images where reasonably possible. It cannot guarantee the recall of printed material or copies others have already saved or shared. The school's privacy information explains its lawful basis for processing personal data; recording parental choices does not itself settle that legal question.

Training, monitoring and review

Online safety is addressed during staff induction, appropriate professional learning and pupil learning. The Principal and safeguarding team review concerns and trends to improve education and safeguards. The policy is reviewed annually and sooner after a significant incident or change in guidance.

Related documents and guidance

Safeguarding and Child Protection Policy; Addressing Bullying Policy; Positive Behaviour Policy; ICT Policy; Social Media Policy; school data protection and staff conduct arrangements.

Guidance considered: DE Circular 2026/17, Child Protection and Safeguarding in Education; DE Circular 2026/16, Guidance on the Use of Mobile Phones in Schools and EOTAS Centres in Northern Ireland; relevant DE online safety guidance; EA online safety resources; UK GDPR and ICO guidance. Current versions should be checked at review.

Appendix A: Pupil online safety agreement (adapt to age)

- I use the internet and school devices only when an adult allows me.
- I keep passwords and personal information private.
- I am kind and respectful in messages and online activities.
- I tell a trusted adult if I see something upsetting, receive an unwanted message or make a mistake.
- I do not take or share photos or videos of others without permission.
- I understand the school may take appropriate action if I misuse technology.

- Pupil name/class: _____

- Pupil signature (if appropriate): _____

- Parent/carer: _____

Appendix B: Staff acceptable use acknowledgement

- I use approved school systems and maintain appropriate boundaries in all digital communications.
- I protect passwords, devices, personal information and pupil images in accordance with school procedures.
- I promptly report safeguarding concerns and suspected security or data breaches through the appropriate channels.
- I do not disclose identifiable pupil information to unauthorised services, including public AI tools.
- I understand that school-system use may be monitored in accordance with notified procedures and applicable law.

- Staff name: _____ Signature: _____ Date: _____