EDENBROOKE PRIMARY SCHOOL

LUCERNA PEDIBUS MEIS

E-Safety Policy

May 2026

1. Introduction

This E-Safety Policy has been developed with reference to the Northern Ireland Department of Education's current guidance and circulars, including Circular 2016/27 - Online Safety, Circular 2011/22 - Internet Safety, Circular 2016/26 - Effective Educational Uses of Mobile Digital Devices and the revised Circular 2017/04 - Safeguarding and Child Protection in Schools (September 2024 update). It also takes account of current Education Authority/C2k guidance and current Northern Ireland online-safety resources, including Safer Schools NI.

The policy should be read alongside Edenbrooke Primary School's Safeguarding and Child Protection Policy, Acceptable Use Agreements, Positive Behaviour and Anti-Bullying Policies and other relevant school policies.

What is E-Safety?

E-Safety is short for electronic safety. This policy highlights the responsibility of the school, staff, governors and parents/carers to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing.

E-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

2. Purpose and Rationale

Edenbrooke Primary School recognises that digital technology and the internet are an important part of children's learning, communication and everyday lives. The school is committed to ensuring that pupils can benefit from technology while being supported to recognise, manage and report online risks.

Online safety is a safeguarding responsibility shared by everyone in the school community. It is not solely a technical matter. This policy therefore sits within the school's wider safeguarding, positive behaviour and anti-bullying arrangements. The Department of Education's safeguarding guidance states that online safety should be clearly reflected in schools' safeguarding arrangements and recommends integrating online safety with safeguarding, positive behaviour and anti-bullying policies.

3. Aims

- Promote safe, responsible, respectful and positive use of digital technology.
- Teach pupils the knowledge and skills needed to manage online risks and develop resilience.
- Prevent and reduce online harm through education, supervision, filtering and appropriate monitoring.
- Ensure online safety is embedded in curriculum and safeguarding practice.
- Ensure staff use approved systems and maintain professional boundaries.
- Ensure safeguarding concerns arising online are reported promptly and recorded on CPOMS.
- Ensure C2k filtering concerns are reported and acted upon.
- Protect personal data, accounts, images and confidential information.
- Review online safety arrangements at least annually and after significant incidents or changes.

4. Scope

This policy applies to pupils, staff, governors, volunteers, students on placement, contractors, visitors, parents/carers and community users when using school devices, networks, accounts or platforms. It also applies to online behaviour outside school where there is a significant connection to the school community, including cyberbullying and safeguarding concerns.

5. Development, Monitoring and review

The school will review this policy at least annually and more frequently where there is a significant new technology, emerging online threat, major change in school practice or serious incident. The review will involve relevant safeguarding, leadership, technical and governance roles.

- Governors will receive appropriate assurance about implementation and significant online safety themes.
- Senior leaders will oversee implementation and ensure appropriate training and resources.
- The ICT co-ordinator will coordinate day-to-day development and awareness.

- The Designated Teacher/Deputy Designated Teacher will lead on safeguarding and child-protection concerns.
- The C2k Manager/ICT co-ordinator will manage liaison with Capita technician and C2k on filtering and technical matters.
- Safeguarding concerns will be recorded on CPOMS in accordance with the school's child protection record-keeping procedures.

6. Roles and Responsibilities

Governors

- Approve the policy and review its effectiveness.
- Ensure online safety is integrated into the school's safeguarding arrangements.
- Receive appropriate information about incidents, training and filtering issues.
- Ensure the school has suitable resources, training and review arrangements.

Principal and Senior Leadership Team

- Have overall responsibility for safe use of digital technology within school.
- Ensure clear reporting routes and effective incident response.
- Ensure staff with online safety/safeguarding roles receive suitable training.
- Manage serious or staff-related incidents under safeguarding, disciplinary and other relevant procedures.
- Liaise with EA, C2k, PSNI and other agencies, where required.

Designated Teacher/Deputy Designated Teacher

- Treat grooming, exploitation, harmful sexual behaviour, sexualised images, sextortion, serious cyberbullying, self-harm risk and other online harms as safeguarding matters where appropriate.
- Ensure concerns are reported promptly and recorded on CPOMS.
- Follow current EA/Department of Education safeguarding procedures.
- Arrange appropriate support and external referral where necessary.

ICT Co-ordinator/E-Safety Lead

- Coordinate online safety education through whole school E-Safety scheme of work.
- Support staff and pupils with advice.
- Review themes and trends in relation to E-Safety and contribute to improvement planning.
- Promote ‘Safer Internet Day’ and online safety key messages through assemblies and lessons.
- Work with safeguarding and technical colleagues.

C2k Manager/ICT Co-ordinator

- Liaise with C2k regarding the managed internet and filtering service.
- Report filtering problems and inappropriate/incorrectly blocked content through the appropriate C2k route.
- Support secure configuration of school devices and accounts.
- Maintain appropriate technical records and support safeguarding investigations where necessary.

All Staff

- Supervise pupil device use appropriately.
- Follow the Staff Acceptable Use Agreement and professional standards.
- Report safeguarding concerns immediately and record them on CPOMS where required.
- Use only approved school systems for professional communication with pupils and families.
- Model respectful, secure and responsible digital behaviour.

Pupils

- Use devices, networks and accounts responsibly.
- Keep passwords and personal information secure.
- Never bypass filtering or security.
- Respect other people's privacy and dignity.
- Tell a trusted adult if something online makes them worried or uncomfortable.
- Never create, request or share harmful or sexualised content.

Parents/Carers

- Support school expectations and encourage safe, respectful technology use at home.
- Encourage children to speak to a trusted adult about online concerns.
- Share significant online safety concerns with the school so that safeguarding action can be considered.
- Follow school arrangements for communication, photography and social media.

7. Teaching and Learning

Online safety education will be age-appropriate and embedded across the curriculum through an E-Safety Scheme of work, assemblies and other planned opportunities.

- Content - recognising harmful, misleading, violent, sexualised or inappropriate material.
- Contact - recognising grooming, manipulation, coercion and unsafe contact.

- Conduct - respectful behaviour, cyberbullying, consent, digital footprints and consequences of sharing.
- Commerce - scams, advertising, hidden costs and in-app purchases.
- Cyber security - passwords, account and device security.
- Critical thinking - checking sources and recognising misinformation, manipulation and AI-generated content.
- Wellbeing - recognising when online activity affects sleep, mood, relationships or learning.
- Emerging technologies - age-appropriate discussion of AI, deepfakes, image manipulation and other developing risks.

Edenbrooke Primary School will use trusted resources from the Department of Education, Education Authority, C2k, Safer Schools NI, CCEA, Childnet and the UK Safer Internet Centre.

8. C2k Filtering, Monitoring and Technical Safeguards

Edenbrooke uses the C2k-managed education network and C2k filtering arrangements for school internet access. Filtering is a preventative safeguard but cannot remove every online risk.

- Pupils and staff will use individual accounts where provided and keep login details secure.
- Unsuitable content or incorrectly blocked educational content should be reported to the nominated ICT/C2k contact, who will refer it to C2k as appropriate.
- Filtering arrangements will be reviewed at least annually and following significant changes or incidents.
- Staff will provide active, age-appropriate classroom supervision of pupil device use.
- The school will use any available technical reports/alerts alongside in-person supervision. Safeguarding concerns identified through monitoring will be referred to the Designated Teacher.
- Users will be informed that school network/device activity may be monitored in accordance with school policy and data-protection requirements.
- New devices, applications and online services should be assessed for safeguarding, privacy and security before use.
- Any alternative internet access must have appropriate safeguarding and filtering arrangements before it is used.

The school will maintain proportionate records of significant filtering/technical checks and actions to support review and governance assurance.

9. Use of CPOMS for Recording and Monitoring

- Edenbrooke Primary School uses CPOMS, a secure online safeguarding and record-keeping system, to log all E-Safety incidents.
- Staff record incidents promptly, attaching any relevant evidence such as screenshots, messages or reports.
- The system automatically alerts relevant members of staff, including the safeguarding team.
- CPOMS enables the school to monitor recurring incidents, identify patterns of concern and ensure timely intervention.
- All records are stored securely in compliance with data protection legislation and are accessible only to authorised staff.

10. Acceptable Use

- Use digital technology lawfully, safely, respectfully and for legitimate school purposes.
- Use school email and approved platforms for professional communication.
- Staff must not use personal email, messaging or social media accounts for private communication with pupils.
- Remote communication with pupils must use approved school platforms and accounts.
- Messages must be professional, appropriate and capable of being reviewed by school leadership.
- Do not send, upload, download or share illegal, abusive, discriminatory, threatening, sexually explicit or otherwise inappropriate material.
- Do not share passwords or use another person's account.
- Do not install unauthorised software or attempt to defeat security controls.
- Respect copyright, licensing and intellectual property.
- Report phishing, scams, suspicious links and other cyber-security concerns.

11. Digital images, Video and Social Media

- Pupil images, video and work will only be published in accordance with the school's consent/privacy arrangements.
- The school will consider pupils' dignity, safety and best interests when using images online.
- School-approved equipment and systems should be used for school photography and recording wherever practicable.

- Images must be stored securely and retained/deleted in line with school arrangements.
- Pupils must not photograph, record, livestream or share images of others without appropriate permission.
- Staff must not post identifiable pupil information on personal social media.
- Authorised staff will manage school social media accounts with appropriate security and editorial oversight.
- The school will consider the risks of AI manipulation before publishing pupil images.
- Misuse or harmful manipulation of a pupil's image will be treated as an online safety/safeguarding concern where appropriate.

12. Data Protection

The school will process personal data in accordance with the Data Protection Act 2018, UK GDPR and applicable EA/school arrangements.

- Personal data will only be collected, used, shared and retained for appropriate and lawful purposes.
- Access to CPOMS, safeguarding records and monitoring information will be limited to authorised staff.
- Staff will use secure, password-protected systems and follow school information security procedures.
- Confidential pupil information must not be stored on personal devices or unauthorised cloud services.
- New digital services, apps, filtering or monitoring systems will be considered for privacy and data-protection implications.

13. Artificial Intelligence and Emerging Technologies

AI can support learning and administration but creates additional risks relating to accuracy, privacy, manipulation, cyber security and safeguarding.

- Pupils will receive age-appropriate guidance on responsible AI use.
- Pupils will be taught that AI output may be inaccurate, biased or manipulated.
- Staff must not enter confidential or sensitive pupil information into unapproved AI services.
- AI-generated or manipulated harmful images involving pupils will be treated as a serious safeguarding concern.
- Deepfakes, nudification, impersonation, blackmail and other AI-enabled abuse will be referred through safeguarding procedures.
- The school will review AI-related risks as technology develops.

14. Cyberbullying

Cyberbullying may include abusive messages, exclusion, threats, harassment, impersonation, gaming abuse, sharing humiliating images or misuse of personal information. It will be managed under the Anti-Bullying and Positive Behaviour Policies and, where appropriate, safeguarding procedures.

15. Mobile Phones and Personal Devices

Pupil mobile phones are discouraged but permitted in limited circumstances, particularly for older pupils travelling home independently, with phones switched off and stored securely during school hours.

- Pupil phones/personal devices must not be used during the school day.
- Where phones are permitted on the premises, pupils must follow the school's current storage arrangements.
- Personal mobile data must not be used to bypass school filtering.
- Photography, recording and livestreaming require appropriate permission.
- Staff personal devices must not be used for private communication with pupils.
- Misuse creating a safeguarding or bullying concern will be managed through relevant procedures.