E-Safety Policy

Adopted by Eversley Primary School Governing Body
Reviewed: January 2024
Review date: May 2024

E-Safety Policy Overview

E-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 safeguarding and awareness for users to enable them to control their online experiences.

The school's E-Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection, security and home learning.

Intent

As a school, we understand that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. We ensure a number of controls are in place at Eversley due to the increased use of ICT to engage and aid learning.

There are three main categories that we focus on to keep children safe online. These include;

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views

Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying

We aim to ensure these areas are covered within our E-Safety policy and are implemented around the school.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

● Voyeurism (Offences) Act 2019

● The General Data Protection Regulation (GDPR)

● Data Protection Act 2018

● DfE (2020) 'Keeping children safe in education'

● DfE (2019) 'Teaching online safety in school'

● DfE (2018) 'Searching, screening and confiscation'

- KCSIE (2023)

This policy operates in conjunction with a number of school policies which include:

- Acceptable Use Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Data Protection Policy
- Model Code of Conduct Policy
- Mobile Phone Policy

Roles and Responsibilities

All staff members are responsible for:

● Taking responsibility for the security of ICT systems and electronic data they use or have access to

● Modelling good online behaviours

● Maintaining a professional level of conduct in their personal use of technology

● Having an awareness of online safety issues

● Reporting concerns in line with the school's reporting procedure

● Following the expectations set out in the Model Code of Conduct

● Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Pupils are responsible for:

● Adhering to this policy, the Acceptable Use Agreement and other relevant policies

● Seeking help from a staff if they are concerned about something they or a peer has experienced online

● Reporting online safety incidents and concerns in line with the procedures within this policy

Good Practice

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 an E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering.
- The school will work with Enfield LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation & Online Protection Centre).

Contents

Eversley Primary School acknowledges the assistance of Kent County Council in providing content in this document.

School E-Safety Policy

Eversley Primary School's Designated Safeguarding Lead will also act as the E-Safety Coordinator as the roles overlap.

Our E-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors in June 2021

The E-Safety Policy will be reviewed annually by the Computing Coordinator or other senior members of staff and monitored by the school's governing board.

Useful contacts:
Chair of Governors – Cheryl Headon
Safeguarding Link Governor – Hadiza Adeyemi
Computing Coordinator – Rhian Goddard

Safeguarding Lead – Flora Georgiou

Why is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in the 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access

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.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools (The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content);
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;

- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

- Enables the continuation of high-quality teaching and learning through the use of online learning platforms, in case of school closures.

The Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

● RSE

● PSHE

● Computing

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world independently and safely regardless of the device, platform or app they are using. Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

● How to evaluate what they see online

● How to recognise techniques used for persuasion

● Acceptable and unacceptable online behaviour

● How to identify online risks

● How and when to seek support and who from

The online risks pupils may face online are always considered when developing the curriculum. We understand that while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Leaders support staff to ensure the curriculum is tailored so pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

● Where does this organisation get their information from?

● What is their evidence base?

● Have they been externally quality assured?

● What is their background?

● Are they age appropriate for pupils?

● Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are worried about. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report to the DSL or deputy

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

 All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the E-Safety coordinator or other senior member of staff.
- All staff must verbally inform a member of the DSL & the Computing Coordinator of any incidents involving E-Safety, in addition to logging this on CPOMS.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail. This must be logged as child on child abuse and reported to a designated safeguarding lead.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space.
- Any photos shared of children without their consent, must be logged as child on child abuse, including cyberbullying via CPOMS

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Safeguarding

E-Safety is a vital part of our safeguarding policy. During safeguarding training and within addition online safety training for staff, we ensure that staff are made aware of and report on the following issues;

- child-on-child abuse, including cyberbullying
- Sexual harassment including non-consensual sharing of nudes and semi-nudes and/or videos and how these can put children at risk
- social media use
- sharing nudes and semi-nudes
- dealing with cybercrime
- county lines
- cybercrime
- Preventing radicalisation
- cybersecurity

Filtering/Monitoring

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.
The school uses a filtered Internet service. The filtering is provided through (London Grid For Learning).

- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform both the Computing Coordinator and a designated safeguarding lead. This should also be logged onto CPOMS.
- If users discover a website with potentially illegal content, this should be reported immediately to the ICT Coordinator. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or LGFL.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Video Conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing 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.
- Mobile phones will not be used for personal use during school time.

The sending of abusive or inappropriate text messages is forbidden. (Please see our Mobile Phone Policy)

Internet Use

- Pupils using the internet are always with a supervised adult, within the ICT suite and with iPad use
- iPads are set up with the LGFL filtering system, in line with the rest of the school's technology
- Impero is used during Computing lessons, which allows for screen mirroring and blocking if a child accesses unauthorised access.
- Staff can access any innapropriate content and are able to see which computer it was accessed from, through the use of Impero
- Staff have a seating plan to enable safeguarding during Computing lessons.

Published Content and the School Website

- The contact details on the website should be the school's address, email and telephone number. Staff or pupil's personal information will not be published.
- The headteacher or nominee 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 and will not enable individual pupils to be clearly identified.

- Parental consent will be sought before any photos of children are published online for any reason.
- Pupils' names will not be used anywhere on the website or blog in association with photographs.
- There is a statement in the school prospectus referring to our policy on digital images of children.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (Please see the GDPR policies)

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enfield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

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 child protection procedures.
- Parents wishing to complain about E-Safety issues should use the established school complaints procedure.
- Discussions will be held with the Safer Primary Schools Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be made aware of the consequences their actions may have

Staff

- All staff will be informed about and given access to the school's E-Safety policy and its importance explained.
- All staff will be made aware of the 4 areas of focus for E-Safety; Conduct, Content, Contact, Commerce
- All staff will be made aware of "child on child abuse" and what this involves within E-Safety via the communication of updated policies

Staff will be made aware of the following issues, updated in KCSIE 2023;

- *Sexual harassment including non-consensual sharing of nudes and semi-nudes and/or videos and how these can put children at risk*
- *social media use*
- *sharing nudes and semi-nudes*
- *dealing with cybercrime*
- *county lines*
- *cybercrime*
- *Preventing radicalisation*

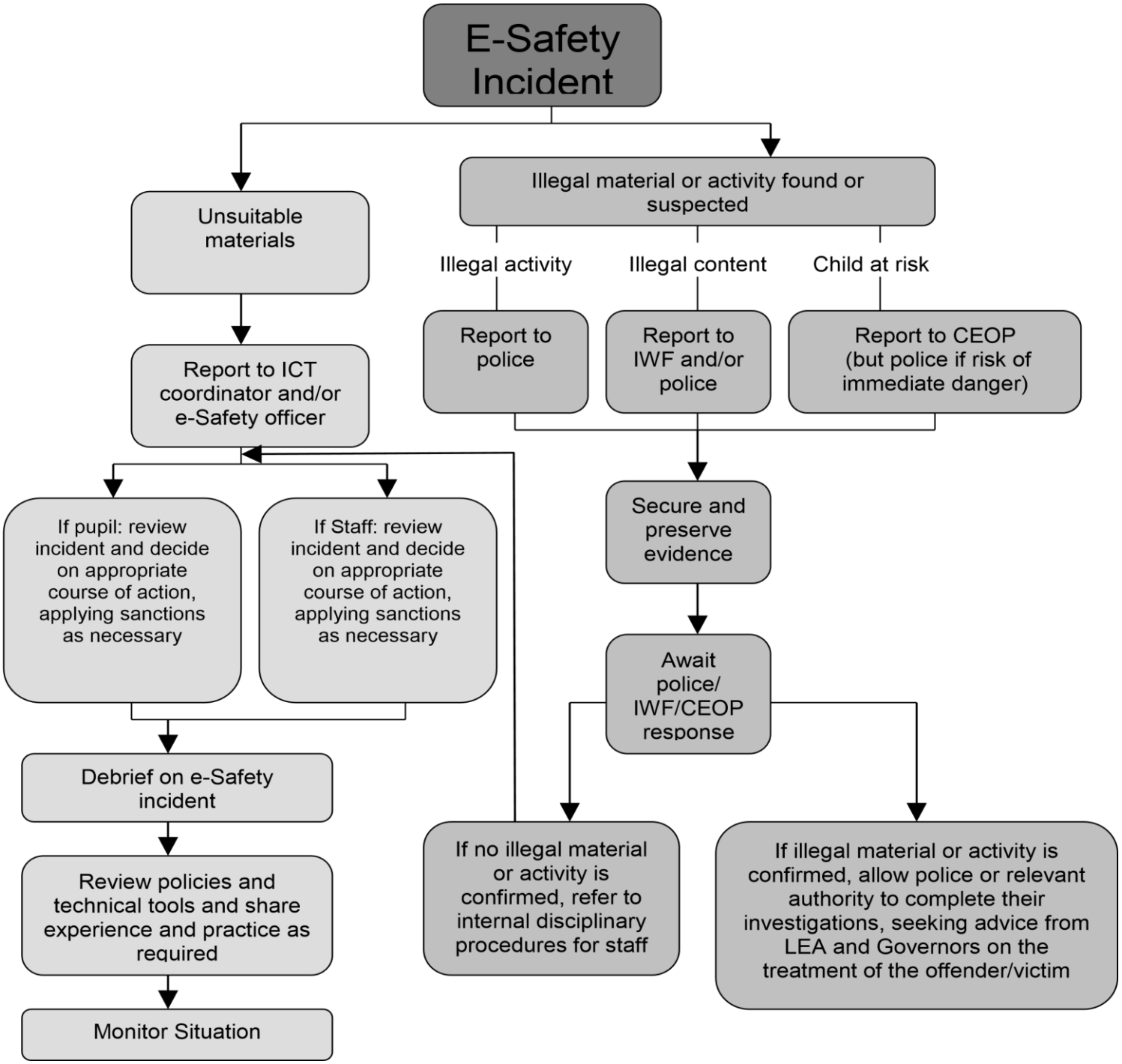
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the school's E-Safety policy in newsletters, the school prospectus and on the school's website.
- E-Safety presentations/workshops organised by school for parents
- Training to be provided for parents where possible

Appendix A

Flowchart for responding to E-Safety incidents in school



Adapted from Becta – E-Safety 2008

Appendix B

Key Stage 2

Think then Click

E-Safety Rules for Key Stage 2

- We ask permission before using the internet.
- We ask permission before using web cameras
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We log out appropriately after each session

E-Safety Rules

These E-Safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through
- The school ICT systems may not be used for private purposes, unless the headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Edit this poster for display near computers.

Appendix C Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure 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 school E-Safety Coordinator or the Designated Child Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote E-Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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.

Appendix D

SMART rules will be used consistently throughout the school and displayed in the ICT suite.