Ermington Primary School

E Safety Policy

Written/Updated:	October 2023
Review Date:	October 2024

Introduction

At Ermington Primary School, we recognise that the internet is an essential resource to support teaching and learning and is a part of the statutory curriculum and a necessary tool for both staff and pupils. As such, we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning both at school and home.
- Use ICT as a tool for communication and understand how to do so in a safe manner.
- Understand the dangers of online communication and know what to do if they feel unsafe when using ICT technology.
- Are prepared for the constant changes in the world of technology and understand how to use all new and emerging technologies safely.

This policy outlines the steps taken by Ermington Primary School to ensure safe internet use by its pupils and staff in school, and also proactively encouraging children to continue to develop a safe approach to ICT use and communication outside of its confines.

Development of this policy

- Headteacher – Mark Mitchell
- Designated Safeguarding Lead and Online Safety Lead – Mark Mitchell
- Computing Lead and E-safety Officer – Clare Starkie-Pell
- PSHE Lead – Kirsty Lavers
- Technician - West Country Schools Trust (WeST)

Schedule for Development/Monitoring/Review

The implementation of this Online Safety policy will be monitored by the: Online Safety Lead Computing Lead Leadership Team (SLT) West Country Schools Trust (WeST)

Monitoring will take place at regular intervals.

Should serious online safety incidents take place, the following external persons/agencies should be informed:

- Headteacher – Mark Mitchell
- Designated Safeguarding Lead and Online Safety Lead – Mark Mitchell
- Computing Lead and E-safety Officer – Clare Starkie-Pell

The school will monitor the impact of the policy using:

• Logs of reported incidents (on CPOMs).

• Monitoring logs of internet activity (including sites visited)/filtering.

• Surveys/questionnaires of students/pupils, parents/carers and staff.

The Law

The e-safety policy has been written by Ermington Primary School using government guidance. However, as legislation is often amended and new regulations introduced, references made in this policy may be superseded. For an up-to-date list of legislation applying to schools please refer to the Department for Education website at: Education, training and skills - GOV.UK (www.gov.uk)

Roles and Responsibilities

E-safety is an important aspect of Safeguarding. As such, the Headteacher and WeSt have the ultimate responsibility to ensure that that the policy and practices are embedded and monitored.

WeST and the Headteacher will:

• Ensure that the E-Safety Policy is implemented, communicated and monitored.

• Ensure that a Computing Policy outlining ICT and e-safety as integral parts of the school curriculum, is implemented, communicated and monitored.

• Ensure that the school has a sufficient filtering software to protect children from potentially damaging material.

The Designated Safeguarding Lead will:

• Ensure that all staff are trained on the aspects of e-safety periodically as part of safeguarding training.

• Include e-safety as part of the Safeguarding Refresher training.

• Ensure that aspects of safety are an integral part of learning as outlined in 'Education for the Connected World -2020 edition'

• Staff are regularly mailed safeguarding updates

• Work with the CAP Team from Devon and NSCC workshops for staff and pupils.

• Parents receive timely advice

• Investigate any reports of cyber-bullying or inappropriate communication and establish learning events where needed.

• Seek advice from WeST or Devon Safeguarding Team when needed.

Teachers and Staff will:

- Read and maintain awareness of the Computing and E-Safety Policies.
- Participate in all e-safety training offered.
- Adhere to the Acceptable Use Agreement which all staff sign.
- Promote and teach e-safety as part of the computing curriculum.
- Monitor and supervise pupils' internet usage and use of other IT resources
- Only download attachments/material onto the school system if they are from a trusted source.
- When capturing images, videos or sound clips of children, only use school cameras or recording devices.
- Never use personal mobile phones or other devices to record images.
- Follow up assemblies around e-safety

Teaching and Learning.

Internet use will enhance learning as follows:

- Pupils will be taught the importance of safe internet use and give clear guidelines and objectives about what is acceptable.
- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience in a safe manner.
- Pupils will be taught the importance of cross checking information before accepting its accuracy, and of following copyright laws.
- All forms of bullying, including cyberbullying will be taken seriously, reported to the Headteacher and logged on CPOMS.

Managing Internet Access

Information system security

- The school's internet access is provided through the South West Grid for Learning (SWGfL) which is designed for pupil use and includes filtering appropriate to the school.
- Computer system security and virus protection will be reviewed regularly by the Technician.
- If staff or pupils discover unsuitable sites, the URL and content will be reported to the computing team who will contact the Technician.

E-mail

- Pupils may only use an approved e-mail account on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal their personal details or those of others, or arrange to meet anyone they have been in contact with.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter on school headed paper.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and school website

- Staff or pupil personal contact information will not be published. (The contact details given will be admin@ermington.devon.sch.uk)
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs that include pupils will be selected carefully so that their image cannot be misused.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs. Website photographs will be selected carefully to ensure individual pupils cannot be identified by name.

Social networking and personal publishing

- The school will control access to social networking sites, and will educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social networking spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networks.
- Schools will ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
- Specific lessons will be included to teach all pupils how to read for information from web resources.
- Staff should exercise caution, sound judgement, and common sense when using social media sites.

• Employees of the school should not communicate with students on roll or former students (until they are over 18) through social media sites, and should exercise extreme caution when befriending or communicating with parents of children enrolled at school.

• No reference should be made via social media to students / pupils, parents/carers/school staff or issues / situations or people related to the school.

• Personal opinions should not be attributed to the school.

• Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.

Managing Filters

• WeST will ensure systems to protect pupils are reviewed and improved.

• If staff or pupils come across unsuitable material or illegal sites, the URL (address) and content must be reported to the Technician and the Headteacher immediately.

• Computing lead and WeST will make regular checks to ensure that filtering methods selected are appropriate, effective and reasonable.

Managing video calls (Zoom,Teams)

• Video conferencing should use the SWGfL broadband network to ensure quality of service and security.

• Parents are present if individual child is at home

Managing emerging technologies

• Emerging technologies will be examined for educational benefits by the Computing Team, and a risk assessment will be carried out before use is allowed.

• Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communication**.**

Pupils are not allowed, therefore, to have mobile phones in school and must hand these in to the office at the start of the school day and not use them on site.

• The sending of abusive or inappropriate text messages or files is forbidden.

• Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.

• Staff must not use their own mobile phones in the presence of pupils and they should be turned off during lesson time. Staff are only permitted to use mobile phones in the school offices or staff room. Visitors receive specific guidance on phone use.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2016.

Policy Decisions

Authorising Internet access

- All staff will be provided with the E-Safety Policy, and its importance explained.
- All pupil internet access will be supervised by an adult.
- Staff development in safe and responsible internet use and on the school Internet policy will be provided as required.

Assessing risks

The school will take reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. WeST cannot accept liability for any material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the Designated Safeguarding Officer.
- Any complaint about staff misuse must be referred to WeST
- Complaints of a Safeguarding nature must be dealt with in accordance with the school's procedures.
- The complaints procedure is available on school websites.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Introducing the E-Safety policy to pupils

- All children begin the academic year learning about e-safety and follow the SMART rules (Safe, Meeting, Accepting, Reliable) to keep them safe when using the internet.
- Resources will be utilised to teach e-safety on a weekly basis, during assembly and both PSHE computing lessons.

• E-Safety rules will be displayed in the main reception and discussed with pupils regularly to remind the children how to use the internet safely and responsibly. Reminders about responsible and safe use should precede internet access.

• Pupils will be informed that network and internet use will be monitored and appropriately followed up.

• E-safety training will be embedded within the computing and PSHE curriculums, covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.

• Resources to support parents at home is signposted on newsletters and on our website and outlines how to stay safe when playing online games.

Staff and the e-safety policy

• All staff will be given the e-safety policy and its importance explained.

• Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

• Staff will use a child friendly search engine when accessing the web with Foundation and KS1 children, however children in KS2 will be taught how to safely search the internet using engines such as Google.

• Children must be monitored by staff at all times, and never left alone when using the internet.

Enlisting parents' and carers' support

• This policy will be available on the school website. Guidance is available on the school website that directs parents to best practise and supporting articles.

• Information will be provided to parents periodically about how to work with the school to ensure e-safety both within school and home.

• A partnership approach with parents will be encouraged.

• The school provide parents with e-safety resources on request.