



Caerau Primary School

E-Safety Policy



Date	Review Date	Co-ordinator	Nominated Governor
September 2022	September 2024	Mrs. J Roche	Mrs. R Goodall

Policy on E-safety

Introduction

This e-safety policy will be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children and home-school agreements.

ICT coordinator and headteacher will act as E-Safety coordinators although the overall responsibility is that of the 'safeguarding persons', also all staff take responsibility for the use and monitoring of ICT within their classes.

Aims

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning.

- Pupils will be given clear objectives for internet use.
- Pupils will be using a wide range of apps and websites to help with their learning.
- Web content will be subject to filters (provided by BCBC).

- Internet use will be embedded within the curriculum.
- Pupils will learn about safety surrounding e-safety and take part in activities promoting 'Internet Safer Day'.
- Pupils will use previous knowledge to help identify and recognise safe websites.

Pupils will develop an understanding of uses, importance and limitations of the internet.

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught about online safety.
- Pupils will use age-appropriate apps.
- Pupils will be taught how to report inappropriate web content.

Pupils will develop a positive attitude to the internet and develop their ICT capability through independent and collaborative working.

- Pupils will use the internet to enhance their learning experience.
- Pupils have the opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely.

- Pupils will be taught about e-safety.
- Pupils will be reminded about the safe use of apps and internet.
- Pupils will take part in numerous activities promoting e-safety.

Published content and the school website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- A designated member of staff will have full control over the website.
- Class teachers will have editing rights to their pages and upload suitable evidence of work and be responsible for accurate and appropriate content.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The consent form will be given out at the start of the school year and be collected by the class teacher.
- The class teacher will keep a record of all consent forms and keep an updated list of children that can or cannot have their image on the school website.

E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network and email usage should be supervised and monitored by a staff member.
- Emails will be Hwb.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.

Internet Access and Learning Platform (Hwb)

- Parents will read and sign an internet access consent form before their children are given access to internet resources.
- Pupils' internet access during school hours will always be supervised by a member of staff.
- A link to online safety (Hwb) will be on the school website on the home page.

Mobile Phones and other handheld technology

- Pupils are not permitted to have mobile phones or other personal handheld technology in school. If such items have to be brought into school by pupils, (i.e. going to a different home after school) they are to be handed to the class teacher at the start of the day to be kept safe until home time.

Systems Security

- ICT systems security will be regularly reviewed with support from BCBC Corporate IT department.

Web Filtering

- The school will work with BCBC Corporate IT department to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to the class teacher or member of staff that is available.

Communication of the e-safety policy to pupils

- Pupils will work on activities on internet safer day and this will be promoted throughout the school.
- E-safety rules will be posted in each room where a computer is used.
- Pupils will be informed that internet and Learning Platform use will be monitored.

Communication of the e-safety policy to staff

- The e-safety is available and accessible to all staff.
- Staff will be informed that internet use will be monitored.

Communication of the e-safety policy to parents/carers

- The e-safety policy will be available on the on the school website under the policy page.
- The internet safety information will be on the home page with a link from Hwb. This covers all the information the pupils and parents need to know and follow.
- Parents will be asked to sign an ICT agreement, when their children join the school.

- The school will communicate and publicise e-safety issues to parents through the school communications and website.

E-safety Complaints

- Instances of pupil internet or Learning Platform misuse should be reported to, and will be dealt with by, the e-safety co-ordinator or headteacher.
 - Instances of staff internet or Learning Platform misuse should be reported to, and will be dealt with by, the headteacher.
 - Pupils and parents will be informed of the consequences of internet and/or Learning Platform misuse.
 - Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
-

Whole-School Responsibilities for Internet Safety

Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to other members of Teaching Staff.
- Ensure that developments at Local Authority level are communicated to staff.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

Governing Body

- E-Safety will be reviewed as part of the regular review of child protection and health and safety policies.
- Support the headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the headteacher and/or designated e-safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Embed e-safety education in curriculum delivery.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within & outside school.
- Take responsibility for their professional development in this area.

Wider School Community

As a school we aim to encourage:

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies. • Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

As a school we aim to encourage:

- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or Learning Platform.
- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.