Capenhurst C.E. Primary School

E-Safety Policy

The Acceptable Use of the Internet and related Technologies

Written by: Mrs Claire Green
Review: September 2025

Policy Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. This is through the application of this policy and a clear programme of study around safe use of technology (see curriculum plans for details).

All staff are made aware of the school Acceptable Use Policies which can be accessed and downloaded via school's staff share server.

Roles and Responsibilities
The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. Governors are reminded of the Seven Principles of Public Office which forms part of the Code of Conduct each governor signs at the start their term of office and the

expectation of professional conduct and confidentiality when sending or receiving emails or information in their capacity as a governor of Capenhurst CE Primary School.

Head teacher and Senior Leaders
The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the computing subject leader.

The Headteacher and Senior Teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff in line with the Allegations Against Staff Policy and LADO Guidance.

Computing subject leader
The Computing subject leader will:

- lead on safety issues across school
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- feedback to the Governing Body on any relevant items, such as safety breaches at governing body meetings
- liaise with the Local Authority ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

Technical staff
School buys into the Local Authority ICT Support through the SBSA. A technician visits the school on a fortnightly basis offering advice and support which may include the following: that the school's ICT infrastructure is secure and is not open to misuse or malicious attack; that the school meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance and that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. School also purchases a filtering package with the advice and support of their ICT technician.

Teaching and Support Staff
All staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Acceptable Use Policy
- they report any suspected misuse or problem to the computing subject leader for investigation and possible action
- digital communications with pupils should be on a professional level and only carried out using official school systems
- use of school laptop for personal purchasing goods and services during non-contact time falls under 'personal use' of electronic resources.

Take advice from your line manager *before* you proceed. Internet Banking facilities should not be accessed whilst using a school connection. When sending e-mails from a school e-mail address or when using school laptops for personal use, staff will ensure that they are mindful of their obligations under the Teachers' Standards, paying particular attention to Part Two Standards for Personal and

Professional Conduct which states that – 'Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach'

Designated Safeguarding Lead

The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Should serious e-safety incidents take place, Cheshire West and Chester ICT Helpdesk (Edsential) Safeguarding Children in Education Team should be informed as appropriate.

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (AUP).

Parents / Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will take every opportunity to help parents understand relevant e-safety issues through parents' evenings, newsletters, letters and the school website.

Educating the school community about e-safety

Whilst regulation and technical solutions are important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This will be provided in the following ways:

- Through the computing curriculum
- Key e-safety messages are to be reinforced through the planned computing curriculum
- Pupils should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information
- Through annual Safer Internet Day activities

Parents and carers sometimes either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, school website
- Parents' evenings
- E-Safety Information sessions as applicable
- Links to advice from specialist providers can be found on the school's website

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. In the main, this will be covered when staff complete their Safeguarding Basic Awareness Training Level 1. Additional information will be shared through e-mails.

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. School is supported in this by their ICT technician. School ICT systems will be managed in ways that ensure that the school meets its e-safety obligations to safeguard and protect its school community. All users will have clearly defined access rights to school ICT systems. All users will be provided with a username and password by the ICT technician.
The "master/administrator" passwords for the school ICT system, used by the ICT Technician must also be available to the Headteacher or another nominated senior leader and kept in a secure place. School will endeavour to avoid one user having sole administrator access. The school infrastructure and individual workstations are protected by up-to-date virus software. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. School uses Egress to send personal data via email to other professionals such as other schools, social care etc.

Curriculum
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of technology across the curriculum. The computing curriculum long term overview clearly identifies what is to be taught to pupils and when. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Use of digital and video images - Photographic, Video
Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites. Staff are allowed to take digital / video images to support educational aims with the proviso that the images are stored only within the school server and not taken away from the school premises.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must ensure that they:

- Take care to always ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Lock their computer when they move away from it.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media; the device must be password protected and offer approved virus and malware checking software.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

- Emerging technologies will be examined for educational benefit and assessed before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The official school email service may be regarded as safe and secure and is monitored by the Local Authority. Egress must be used when sending personal data via email, even when this is to other school in the same school.
- Users need to be aware that email communications may be monitored
- Users must immediately report to the nominated person the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students/pupils or parents/carers must be professional in tone and content.
- Members of staff at the school should not be interacting with students electronically in any form.
- 'Open' communications such as blog comments, social media posts should be appropriate to your professional remit*. If using a personal account, you should make clear that all comments are your own.*
- Staff social networking profile should be completely unavailable and staff should make any avatars 'appropriate'.
- 'Groups' you join on social networking sites may be seen. Make sure they and any public comments you make reflect positively on you and your profession. Make sure any groups you join cannot have racist, sexist or any other inappropriate overtones

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of technology, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or deliberate misuse. All apparent or actual incidents of misuse or illegal activity will be recorded, and advice sought from the appropriate department of the local authority as the correct course of action thereafter.

Schedule for Monitoring and Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.