CASTLE PRIMARY SCHOOL

E-safety Policy

E-Safety Lead – Miss J Mason

REVIEW DATE: SEPTEMBER 2025
(Sooner if required)

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

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 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.

Policy Links

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Child Protection, Safeguarding Children, Curriculum, Data Protection and Security, Confidentiality.

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 e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband for learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-safety considers the following technologies:

- PC's, laptops, tablets, webcams, digital video equipment, mobile phones, portable media players, games consoles and personal digital assistants.

All persons either using technology or supervising the use of technology are required to abide by this policy.

E-safety requirements relate to school-owned technology and also to personal technologies.

E-safety requirements are applicable during the times whereby the school is open; this applies to term-time, extended school events, lettings for community use. It is also relevant to residential/off-site events e.g. school trips and visits.

Designated Person for E-Safety Policy

The school will appoint an E-Safety Officer. In many cases this will be the Designated Child Protection Officer as the roles overlap.

The E-Safety Officer is Jill Mason supported by Hannah Bours in her role Deputy Child Protection Officer.

Our E-Safety Policy has been agreed by the Senior Leadership Team and approved by the Governing Body.

Content, Contact, Conduct and Commerce

An important step in improving online safety at your school is identifying what the potential risks might be. KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the 4 Cs of online safety.

Internet: The Benefit to Education

Benefits of using the Internet in education include:

- Fully supports the school's implementation and delivery of a creative Curriculum to enhance learning opportunities

- Access to world-wide educational resources

- 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 DfE; access to learning wherever and whenever convenient

- 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 safety rules 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

Our school will comply with copyright law.

The school will maintain a current record of all staff and pupils who are granted Internet access.

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

Parents will be informed that pupils will be provided with supervised Internet access.

Safeguarding Children and Child Protection

This policy is an extension of the safeguarding children and child protection policies. Caution is expressed to the whole school community as regards child safety in the virtual world as well as the real world. Social networking sites, the uploading of inappropriate web content and cyber-bullying are issues that adults must ensure vigilance and ensure appropriate means are put in place to safeguard and educate our children. It is expected that children are able to develop their own protection strategies for when adult supervision and technological protection are not available.

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 Officer.
School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

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.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
Whole class or group e-mail addresses should be used in school.
Staff should not access personal email accounts using school equipment.
For all school business, school email accounts should be used.
Staff using personal devices (ipads and mobiles) can access personal email account in school in their own time.
E-mails sent to external organisations should be written carefully and professionally, 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.
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.

Filtering

The school will work in partnership with the Local Authority, and the Internet Service Provider to ensure filtering systems are as effective as possible. Filtering will be actively monitored with issues dealt with accordingly. Any breaches in use will be sanctioned as necessary and if needed reported to the Governing Body, Trust and Local Authority. We use SENSO filtering and monitoring software.

Video Conferencing

(At present video conferencing is not undertaken at Castle Primary)
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 lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
Photographs of children **must not be taken** on a mobile phone.

Published Content and the School Web Site

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.
The SLT 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 or their image misused.
Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
Work can be published with the permission of the pupil and parents.

Information System Security

School IT systems capacity and security will be reviewed regularly.
Virus protection will be installed and updated regularly.
Security strategies will be discussed with the Local Authority.
Regular Internet safety guidance will be given to the children (at least annually).

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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 The Learning Partnership Trust can accept liability for the material accessed, or any consequences of Internet access.
.

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 Head Teacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of the complaint's procedure.
Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils
Rules for Internet access will be posted in all classrooms and spaces where IT equipment is used.
Pupils will be informed that Internet use will be monitored.

Staff
All staff will be given the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Parents
Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Flowchart for Responding to E-Safety Incidents in School

E-Safety Incident/Unsuitable materials
Report to Head Teacher or SLT
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
Inappropriate Activity
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Contact Safeguarding Children Advisory Service if deemed appropriate
Implement changes
Monitor
Review policies and technical tools

Information and posters to assist in the implementation of this policy are attached.

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 email, personal publishing, blogs or messaging.
- The school IT systems may not be used for private purposes, unless the head teacher 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 web-sites, 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.

Blogging Rules

- When commenting remember to use only log in names that appear on your blog page. No surnames.
- Keep safe- don’t reveal any personal information.
- Do not upload any pictures or photographs of yourself or family.
- No text talk- write in full sentences and read your comment back before submitting.
- Be polite- don’t post anything that could hurt or offend anyone.
- After you have finished commenting, ensure you log out carefully.
- Keep your password secret- only share it with those who help you on the blog.
- Always show respect- be positive if you are going to comment.
- Remember the purpose of your class blog- it is not a place to chat.
- All comments posted will be moderated by class teachers before they are uploaded to the blog.

For more information about staying safe online, visit
www.thinkyouknow.co.uk

Happy blogging!

Staff/Governors/Visitors Acceptable User Code of Conduct

To ensure that staff/Governors and visitors are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.
Staff/Governors and visitors 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/visiting role.

I understand that school information systems may not be used for private purposes, without specific permission from the Head Teacher.

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 Lead or the Designated Child Protection Lead or a member of the SLT.
.
I will ensure that any electronic communications with pupils are compatible with my professional/visiting 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.

Signed ______________________ Print Name ___________________________

Designation ______________________________ Date __________________

Key Stage 1

____

Think before you Click!

Rules to help me to stay safe on the Internet

I will only use the internet when an adult is with me

I will click on the buttons or links when we know what they do.

I will only use internet sites that an adult says I can access

I will always ask if I get lost on the Internet.

I can send and open emails together.

I will never give out personal information or passwords.

I can write polite and friendly emails to people that we know.

I will never arrange to meet anyone I don’t know.

I will not open e-mails sent by anyone I don’t know.

I will not use Internet chat rooms.

Signed ______________________ Date _____________

Key Stage 2

____

Think before you Click!

E-Safety rules to keep me safe on the internet

I will ask permission before using the Internet.

I will only use websites that an adult has chosen.

I will tell an adult if I see anything I am uncomfortable with.

I will immediately close any webpage I am not sure about.

I will only e-mail people an adult has approved.

I will only send e-mails that are polite and friendly.

I will never give out personal information or passwords.

I will never arrange to meet anyone I don’t know.

I will not open e-mails sent by anyone I don’t know.
I will not use Internet chat rooms.

Signed ________________________ Date _________________