ROSSMORE SCHOOL

E-SAFETY POLICY

Date of Policy: September 2024
Date of Review: September 2025

At Rossmore, we understand that computer technology is an essential resource for supporting, teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. Rossmore School's E-Safety Policy has been written by the school, drawing on current government guidance. It has been agreed by senior management and approved by the governors. The E-Safety Policy and its implementation will be reviewed annually.

1. Teaching and Learning

Why the internet and digital communications are important:

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils use the internet widely outside of school, and need to learn how to evaluate internet information and to take care of their own personal safety and security whilst online.
- 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 functions.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and effective curriculum practice;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DfE;
- access to learning wherever and whenever convenient;
- access to the use of the school's website. This will encourage pupils and give them the opportunity to blog and have educational discussions in a supported and controlled online environment.

How will internet use enhance learning at Rossmore School?

- The school Internet access will be designed expressly for pupil use and will include 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- Staff will guide pupils to online learning activities that will support the learning outcomes planned to suit the pupils' age and maturity.

Evaluation of Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report internet content they find unpleasant.

2. Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media, such as memory sticks and CD-ROMs, may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

E-Mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, unregulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, children at Rossmore School do not have access to a school email address. So that the children can experience using email, a generic class or project email address would be set up through a controlled APP and would be carefully monitored. This way, we can achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- Pupils may only use approved e-mail accounts on the school system or selected APP's.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils are taught how they must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils may not access personal email accounts in school, but as
- E-mail sent to an external organisation is 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.
- The sending of abusive or inappropriate email messages is forbidden.

Published content and the school website

The school web site/Learning Platform - celebrates pupils' work and promotes the school.

- The point of contact on the Web site is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.
- The Headteacher and Admin team take overall editorial responsibility and try to ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils are selected carefully so that individual pupils cannot be identified and their image misused. Consider using group photographs rather than full face photos of individual children.
- Pupils' full names are not used anywhere on the Web site or other online space, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents/carers.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.
- Pupil image file names will not refer to the pupil by name.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils will only use moderated social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff are aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable

material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger and many others.

- Staff will not under any circumstances mention any references to their working lives on any social media.

Managing filtering

The school works in partnership with parents, the LA and DfE to ensure that systems to protect pupils are reviewed and improved.

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the school Bursar.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected (Securus) are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection Centre.

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.
- The senior management team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Staff all have access to a lockable locker where they will keep their mobile phone's during school hours.
- Staff will be issued with a school phone where contact with pupils or parents is required, e.g. school trips to include residential.
- The appropriate use of Learning Platforms will be discussed as the technology continues to be available within the school.
- No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks. ICT technicians will inform pupils and staff members of this rule before they can use school-owned devices away from the premises.
- All school-owned devices are password protected – these passwords will be changed regularly to ensure their security.
- All mobile devices and hand-held computers will be fitted with tracking software to ensure they can be retrieved if lost or stolen.
- To protect, retrieve and erase personal data, all mobile devices and

hand-held computers will be fitted with software to ensure they can be remotely accessed.

- Rossmore's ICT technician will review all mobile devices and hand-held computers on a monthly basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.
- APP's and/or computer programmes will be reviewed before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician. APP's will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection.
- Important folders, e.g. those including pupils' medical records, will be password protected to ensure their security.
- Firewalls will always be switched on and checked fortnightly by the ICT technician.
- Staff will report any viruses to the ICT technician immediately.

3. Policy Decisions Authorising

Internet access

- The school allocates Internet access for staff and pupils on the basis of educational need. Parental permission is required for each pupil.
- All staff must read and sign the 'Acceptable use of ICT policy before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to the school's ICT systems.
- Parents are informed that pupils will be provided with supervised Internet access and are asked to return a consent form.
- Any person not directly employed by the school will be asked to sign an 'Acceptable use of ICT' policy before being allowed to access the internet from the school site.

Assessing risks

The school will take all 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. The school cannot accept liability for any material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly. The headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act.

Complaints procedures

- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- 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 referred to the school Designated Safeguarding Lead and dealt with in accordance to school child protection procedures
- Pupils and parents will be informed of consequences for pupils misusing the Internet. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions are in place, linked to the school's behaviour policy.
- Sanctions available include:

- interview/counselling by Headteacher informing parents or carers, removal of internet or computer access for a period.

- Pupils and parents will be informed of the complaints procedure (see school Complaints Policy)
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with other safeguarding issues, there may be occasions when the police must be contacted.

4. Communications Policy

Introducing the E-Safety Policy to pupils

- E-Safety rules will be posted in rooms where computers are used and discussed with the pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in E-Safety will be delivered through programme called E-aware.
- Instruction in responsible and safe use will precede Internet access.
- E-Safety training will be embedded within the ICT scheme of work or the curriculum.
- The E-Safety officer will hold an assembly at the start of the school year explaining what a phishing email/ website may look like. The assembly will be given to children of appropriate age and may include the following:
  - Determining whether or not an email address is legitimate
  - Knowing the types of address a phishing email could use
  - Asking “does it urge the recipient to act immediately?”
  - Checking the spelling and grammar

Staff and the E-Safety policy

- All staff will be given the E-Safety policy and its application and importance explained.
- Staff should be aware that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will use a child friendly safe search engine when accessing the web with pupils.

Enlisting parent/carer support

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents are also advised to check if pupils' use elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents'/Carers' attention will be drawn to the school's E-Safety

Policy in newsletters and on the school Learning Platform.

- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents will be encouraged.
- The school will maintain a list of E-Safety resources for parents/carers.
- The school will ask new parents to sign the parent/pupil agreement

Date of Policy: September 2024
Date of Review: September 2025

Rossmore School

ICT Acceptable Use Policy

Rules for Students and Staff

The school computer system provides Internet access to students and staff. This Responsible ICT Use Policy will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or staff professional development.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Do not send, attempt to access, save or display offensive messages or pictures. If any such material accidentally appears inform a member of staff immediately.
- The use of public chat rooms is not allowed.
- The security of ICT systems must not be compromised, do not attempt to access areas that you are not allowed to, this is hacking.
- Irresponsible use of the ICT facilities may result in the loss of Internet access either on a temporary or permanent basis.
- Treat the equipment with respect, always inform a teacher if *"there* is something wrong, never attempt to fix a problem yourself.
- Anyone caught purposely damaging equipment will be charged and punished.

The school may *exercise* its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Date of Policy: September 2024
Date of Review: September 2025

Dear Parents
Responsible ICT Use

As part of your child's curriculum and the development of ICT skills, Rossmore School provides supervised access to the Internet. We believe that the use of the World Wide Web and E-Mail is worthwhile and is an essential skill for children as they grow up in the modern world.

Please would you read the attached ICT Acceptable Use policy then sign and return the consent form so that your child may use Internet at school.

The school takes positive steps to try and ensure that pupils do not have access to undesirable material. Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

Please take time to discuss the attached policy with your child and then complete, sign and return to your child's teacher.

As a user of school and/or e-learning foundation ICT equipment I agree to comply with the above Acceptable Use Agreement.

Pupil Name Signed
Parent name Signed
Year Group
Teacher
Date .

Date of Policy: September 2024
Date of Review: September 2025

Parent's Consent for Web Publication of Work and Photographs
(please tick appropriate box)

- I agree that, if selected, my son/daughter's work may be published on the school Learning Platform. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not identify individuals and that full names will not be used.

I do not want my child's work or photograph to be published on the school's Learning Platform.

Signed (Parent):.
Date: