

e-Safety Policy

What is e-Safety?

All people working in a school, whether adult or child, have a duty to be aware of the security risks and problems that working with Information and Communication Technologies and data can pose. These issues are known as 'e-safety'.

E-safety is not limited to school premises, school equipment or the school day. Neither is it limited to equipment owned by the school. Changing technology and ways to communicate mean that data and IT systems can be more widely, quickly and easily accessed.

A duty of care

There is a responsibility for staff and students to be aware of e-safety at all times, to know what is safe and acceptable.

E-safety is a child protection issue and relates to other policies including those for bullying and Child Protection procedures. E-safety issues occurring outside of school may be dealt with through these procedures.

Why protect data?

As well as resources and files supporting the running of the school, Ratton holds a wide range of personal data on students, staff and other stakeholders. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss or misuse of personal/school data could result in legal liability, adverse media coverage and significant damage to operations of Ratton.

This policy

Ratton School is responsible for the security and protection of personal data and ICT systems. This policy sets out the measures and methodologies in place to ensure that security is adequate and there is compliance with current legislation.

This policy has been written by the school, building on County Council, BECTA and government guidance. It has been agreed by senior leadership and approved by governors.

This version of the policy approved by Governors on: 23rd June 2009

This policy will be reviewed annually.

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 will provide students with Internet access and digital communication technologies as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Safe use of the Internet

- School Internet access will include content filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the Internet/digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective and legal use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Internet content

- 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.

Managing technologies

Information system and network security

- School ICT system and Network security will be reviewed regularly (at least six monthly). Any resulting action will feed into ICT Development Plans.
- Virus / malware protection and Firewall are installed and updated regularly.
- Wireless networks will be encrypted to a safe standard
- Staff and student will be forced to change their password on a periodic basis.
- Security strategies will be discussed with the Local Authority to safeguard protection.
- Staff and students must keep passwords secure and personal. Under no circumstances must passwords be shared or distributed to others.
- Staff and students must log out of systems when not in use.
- Sanctions will apply to students or staff who deliberately bypasses security systems in order to gain unauthorised access to data or other digital resources.

E-mail

- Students and staff may only use approved e-mail accounts.
- Staff must not use school e-mail accounts for personal or commercial use.

Published content and the school web site

- Staff or student personal contact information will not be published. The contact details given online should be the school office.
- The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school Web site or other online space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site or other online space.
- Work can only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- The school will control access to social networking sites and educate students in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing filtering

- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.

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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

Policy Decisions

Authorising ICT access

- All staff must read and accept the 'Acceptable Use of ICT - Staff Guide' document.
- All students must read and accept the 'Acceptable Use of ICT - Student guide' document.
- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. *Note: upon agreement of this policy this will need to be done retrospectively for current staff*
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents/carers will be asked to sign and return a consent form.

Handling breaches of e-safety

- All breaches of e-safety, whether by direct observation or disclosure will be taken seriously.
- E-safety breaches will be investigated by the Network manager and ICT Support team, with referral to a senior member of staff. If appropriate to circumstance, evidence of the incident will be preserved by the Network manager.
- Complaints of a child protection nature will always be dealt with in accordance with school child protection procedures.

Data and data protection

Adhering to the Data Protection Act

Ratton School will comply with the Data Protection Act and follow the guidelines for good information handling. Personal information must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than necessary
- processed in accordance with the individual's rights
- kept secure
- not transferred to countries outside the European Economic Area, unless there is adequate protection.

Furthermore, there is a requirement under the Data Protection Act to notify the Information Commissioner's Office (ICO) of any personal information that Ratton holds. This covers information on pupils, staff and governors. A registration fee and renewal will be done annually.

Informing parents about data held

- A 'Fair Processing Notice' will be given to all parents and carers explaining that personal data is held, along with an explanation about how the data will be used.
- A publication scheme on information available under the Freedom of Information Act 2000, will be available on the Ratton School website.

Backup of school data

- A full data backup of all school files/data performed daily
- A full data backup will be archived every two weeks (tapes are recycled after a period of time)
- Backup tapes will be stored on-site in two separate secure fireproof safes
- Backup tapes will never be stored or taken off-site

Communicating e-Safety

Students and e-safety

- Students will be made aware of e-Safety rules and a programme of training in e-safety implemented into the curriculum.
- Students will be informed that network, Internet and ICT use will be monitored.

Staff and e-Safety

- Training will be provided to relevant staff and governors as need arises.
- All staff will be given the School e-Safety Policy and Acceptable Use guidance and their importance explained.
- Induction procedures for new staff will include e-safety and acceptable use
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff should understand that online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy and Acceptable Use guidance in newsletters, the school brochure and on the school Web site.
- The school will provide e-safety resources and information for parents/carers.