

ETTINGTON CE PRIMARY SCHOOL



E-SAFETY POLICY



OVERVIEW

- E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Our e-Safety Policy has been written by the school, building on the Warwickshire e-Safety Policy and government guidance.
- The school's e-safety policy will operate in conjunction with other policies including those for ICT, Student Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.
- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.

TEACHING AND LEARNING

Why Internet use is important

- With technology growing and developing at a fast pace, pupils will use the Internet widely outside school and will need to evaluate Internet information and take care of their own and others safety.
- The Internet is an essential element for education, business and social interaction.
- The school has a duty to provide children 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.

Internet use will enhance learning

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of the child.
- 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
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

- Information system security School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- 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 email communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

- The Head Teacher, admin staff and ICT co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.
- 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.
- Pupils' full names will not be used anywhere on the school website
- particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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 or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Emerging Technologies

- Mobile phones must be switched off and should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

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

ICT access

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user
- E-safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- Parents will be asked to sign and return pupils acceptance agreement form.
- The school will take all reasonable precautions to ensure that users access only appropriate 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 school

Managing Internet Access

- Information system security School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- 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.
- E-mail sent to an external organisation should be 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.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- 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.
- Pupil's work can only be published with the permission of the pupil and parents.

Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.
- If staff or pupils discover an unsuitable site, it must be reported to the named e-Safety person.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Mobile phones must be switched off when entering the school building and only used in Staff area. Mobile phones should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.

POLICY DECISIONS

Authorising Internet access

- All staff must read and sign the "Acceptable ICT Use Agreement" before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school or WCC can not accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the head teacher.
- 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 complaints procedure.

Community use of the internet

- Pupils are encouraged to continue their safe and responsible use of the Internet outside of school.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

- The school will liaise with local organisations to establish a common approach to e-safety.
- E-Safety will be revised at the start of each school term; classrooms should have rules of internet safety displayed clearly by computers.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Staff and the e-Safety policy

- 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 is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parents will be given e-Safety leaflet
- Internet issues will be handled sensitively, and parents will be advised accordingly.