

Riverside Primary School

E-Safety Policy

September 2022

Reviewed



Riverside Primary School

E-Safety Policy

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.

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

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

Effective Practice in e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; 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 including the effective management of filtering through ICT services;
- A school network that complies with the National Education Network standards and specifications.

School e-safety policy

Writing and reviewing the e-safety policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

The ICT Co-ordinator has overall responsibility for E-Safety within the school. Our Schools' E-Safety Policy has been carefully reviewed.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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 will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This will be managed by LA ICT services.
- 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.
- Selected pupils will be taught and permitted to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught procedures for reporting unpleasant Internet content.
- Pupils will be taught to use Google Safe Search.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with North Tyneside LA.

E-mail

- Pupils may only use approved e-mail accounts (set up by Paul Greatbatch using @riversdeprimary.org.uk) as requested. Pupils are only permitted to email within the school, or with the class teacher's permission, via a class account when emailing outside organisations
- Staff have been issued with Gmail accounts for school use. Home/personal email accounts are not to be accessed in school.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details or those of 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.

Published content and the school web site

- The contact details on the Website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully to ensure that individual pupils cannot be identified. Pupils' full names will not be used anywhere on the Web site, 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 only be published with the permission of pupils concerned and their parents/carers.
- Parents will be clearly informed of school policy on image taking and publishing.

Social networking and personal publishing

- Access to social networking sites is not permitted within pupil accounts, this can be accessed via staff accounts in school. Social media is used as a platform for communication with parents.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location, when accessing social networking sites out of school.
- Pupils will be encouraged to use nicknames and avatars when using these sites.

Managing filtering

- The school will work with the LA, DfES and BECTA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable materials, the site must be reported to the IT Technician, via online form.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 used by pupils will not be permitted in school.
- Appropriate use of the Internet will be discussed as the use of the technology develops within school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff/visitors 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, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to prevent access to unsuitable material. However, it is not possible to guarantee that such material will never appear on a computer connected to the network. The school cannot accept liability for any content accessed, or resulting consequences.
- 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 a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- 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.
- Pupils and parents will be informed of consequences for misuse of the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in rooms where computers are used by pupils. These rules will be discussed with the pupils regularly.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed.
- E-Safety training will be embedded within the ICT and PSHE curriculum.

Staff and the e-Safety policy

- All staff and visitors 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.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy via newsletters, the school prospectus and the school Web site.
- A list of e-Safety resources for parents/carers will be maintained by the school.
- New parents will be asked to sign the parent/pupil agreement when they register their child with the school.

Review Date: September 2024