E-Safety and Acceptable Use Policy

Internet development is constantly evolving into ever more innovative areas with many websites enabling amazing creativity and interaction between peers. Unfortunately though, there are times when internet use can have a negative effect on children. Romiley Primary School recognises the potential dangers and has set out to ensure safe usage by all.

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 is provided by Zen and backed up by Plusnet. The system is manged by RP Technic on behalf of Romiley Primary School and includes filtering appropriate to the age of pupils. FortiGate is the filtering service approved by BECTA for use in school. An additional filtering set is available in school administration networks only and enables staff access to additional resources.
- 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 taught how to evaluate Internet content

- SMT should ensure that the use of Internet derived materials by staff and by 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 as part of our 'SMART' e-safety digital literacy teaching.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection with Fortigate will be installed and updated regularly (usually hourly)
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system for internal communication.
- 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Staff e-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

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 Headteacher 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 parent's permission sought.
- Pupils' full names will not be used anywhere on the Web site or electronic newsletters including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained at entry to school before photographs of pupils are published on the school web site.

Social networking and personal publishing on the school shared network

- FortiGate will normally 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 must not place personal photos on any shared documents provided in the shared network.
- Students should be encouraged to invite known friends only and deny access to others (Year 5/6 cyber safety lessons)

Managing filtering

- The school will work in partnership with Stockport LA and RPtechnic to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Headteacher who will notify RPtechnic at Richard.Fox@rptechnic.co.uk who will make the human intervention adjustments necessary.

Managing videoconferencing

- IP video conferencing will use the educational broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call, including calls originating within the school.
- Videoconferencing 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 during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required as part of a demonstration of mobile communication.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All authorised staff issued with login details must read the e safety e-safety policy before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupils must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

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 Stockport LA can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The annual pupil survey results will be shared with the Headteacher

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.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

Introducing the e-safety policy to pupils

- e-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.

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.
- The RPtechnic managed filtering system and monitoring of ICT use will ensure that FortiGate is updated hourly regarding URL filtering, categories and antivirus.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parents and carers will from time to time be provided with additional information on e-safety.

Expectations for Internet use

(Acceptable Use Policy)

- We expect everyone to be responsible for their own behaviour on the Internet, just as they are anywhere else in school.
- Pupils must always ask permission before using the Internet and have a clear idea why they are using it.
- Children and staff will never reveal personal details, home addresses and telephone numbers on the web or in dialogue with other Internet users.

- Children are only permitted to use email under supervision and if part of a lesson. All email will be moderated and monitored by the class teacher. The use of unfiltered web-based email (such as Hotmail) is not permitted.
- Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from their teacher. This may only occur within privately created chat rooms with closely guarded passwords.
- The use of public chat rooms and Internet Messaging Services is prohibited.
- The use of social networking sites such as MySpace are not generally appropriate to primary education and the use of the Internet for such purposes is not currently permitted.
- Computers should only be used for schoolwork and homework.
- Files may only be downloaded by staff, or children under supervision.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any child finds themselves uncomfortable or upset by anything they discover on the Internet, they will turn off the monitor immediately and report it immediately to the supervising adult. (Any adult should report it Head Teacher immediately. Arrangements can then be made to request that FortiGate block the site via RPTechnic).

In Reception, children may log on using a year group login, but from Year 2 upwards, pupils should generally only access the network using their own personal login. No network user should access other people's files unless permission has been given.

Any infringement of these conditions of use will be dealt with by the class teacher/Head Teacher as appropriate and sanctions may apply. Parents will be informed in accordance with the signed acceptable use agreement.

This policy has been created using the research and relevant guidelines of: -

BECTA (British Educational Communications and Technology Agency- www.becta.org.uk

Reviewed Wednesday 17th January 2018