Rainow Primary School

Caring, Learning, Achieving.

e-Safety Policy

Members of staff responsible:	**Computing SL / Headteacher**
Date approved by Governors:	**Summer 2017**
Date to be reviewed:	**Summer 2020**

Introduction

This e-Safety Policy encourages the responsible use of electronic communication through education and good practice. It highlights the benefits and risks of these technologies and sets expectations of behaviour. The guidelines set boundaries that enable control of the on-line experience without denying children the opportunity to broaden their learning experience. This document focuses on those factors under control of the school.

Good Habits

e-Safety is a core element of the school's Safeguarding system and online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 provided by the Local Authority, including the effective management of content filtering. (Smoothwall – restrictive settings for different user profiles)

Scope

This policy shall be:

- Checked annually in tandem with an e-Safety audit;
- Form the basis of good e-Safety practice within the school.

Teaching and Learning

E-safety should be a continuing focus in all areas of the curriculum and staff should reinforce e-safety messages, wherever possible, in the use of Computing across the curriculum.

- The school will provide Internet access as part of the learning experience provided by an educational broadband network.
- The school's Internet access will be employed expressly for education and will include age-appropriate content filtering.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and learning activities. The school will also promote and take part in the annual Safer Internet Day https://www.saferinternet.org.uk/ which takes place in February each year.
- A planned online safety curriculum should be provided as part of Computing / PHSE /other lessons and should be regularly revisited throughout the academic year.

- 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 to be critically aware of the online materials they read and shown how to validate information before accepting its accuracy.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with the law.
- The Computing Subject Leader will ensure that this policy is applied.
- The Digital Leaders, selected pupils from KS2 who champion, support and help lead Computing in school, will seek to model and promote good internet use.
- School will seek to provide information and awareness to parents and carers through letters and newsletters, parent workshops and reference to relevant online guidance provided by the school website.

Pupil Responsibilities

- Pupils must keep their personal passwords safe and not share them with other pupils.
- In school, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive messages or see inappropriate materials.
- Pupils should ask permission from the supervising teacher before making or answering a voice or video conference.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils should be encouraged to invite known friends only and deny access to others when using social networking sites.
- Pupils must not arrange to meet anyone without specific permission.

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.

Published Content

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2003.
- 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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site**.**
- Pupils' full names will not be used anywhere on the web site.
- Social networking sites will be filtered or blocked at the discretion of the head teacher.
- Newsgroups/forums will be blocked unless a specific use is approved.

- Staff are advised of the possible consequences and repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils.

Filtering Content

- The school will work with the LA to ensure systems to protect pupils are reviewed and improved. We currently use 'Smoothwall' with restrictive settings for different user profiles.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator and the ICT co-ordinator both of whom should be known to all staff members.
- Virus protection will be installed on every computer and will be set to update automatically at least once a week.
- IP video conferencing should use the educational broadband network to ensure quality of service and security.

Introducing 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 be used only at the discretion of the head teacher.
- The use of portable media will be monitored closely as potential sources of computer viruses and inappropriate material.
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students. Staff will use the school phone where contact with pupils is required.

Policy Decisions

- All staff must read and sign the *'Acceptable Use Policy'* (AUP) agreement before using any school ICT resource.
- Pupils must read (or have read to them) and agree to the *'Pupil Acceptable Use Policy'.* (AUP)
- The Digital Leaders will take a role in reviewing the *'Pupil Acceptable Use Policy'* and will also present an assembly to launch it annually.
- Parents will be asked to agree to and return a *'Parent/Carer Acceptable Use Policy'.*
- Volunteers will be asked to agree to and sign a *'Volunteers' Acceptable Use Policy'.*
- 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. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate sites will be immediately reported to the local authority ICT team.
- The school will audit ICT provision annually to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling Incidents

- Incidents of Internet misuse, either by pupils or staff, will be dealt with by the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection/safeguarding procedures.

Policy Communication

- e-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- All staff will be given access to 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.
- Parents' will be advised that the e-Safety policy is published on the school web site and is also available in hard copy by application to the school.

Useful Advice/Support

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
https://www.saferinternet.org.uk/
http://swgfl.org.uk/products-services/esafety/resources
https://360safe.org.uk/

This policy should be read in conjunction with the following policies:

Safeguarding Policy for Children and Young People
Child Protection
Social Media
Behaviour, Discipline and Anti-bullying
Computing and ICT
Data Protection

See also the following referenced school documents:

Rainow Pupil Online Safety Rules (displayed around school and on the pupil log-on screens)
Staff / Parent/ Pupil Acceptable Usage Policies (available on request from the school office)