



Reviewed on:	November 2018
Next review:	November 2021
Staff Responsibility:	Sadia Riaz
Linked policies:	Computing Policy Safeguarding and child protection Policy Anti-bullying Curriculum Data protection and security.
Signed by chair:	L. Rowbotham
Date:	November 2018

Boarshaw Community Primary School **E-Safety Policy**

Introduction

E-Safety Policy E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Safeguarding, Computing, Anti-Bullying, Curriculum, Data Protection and Security. The schools e-safety lead is Sadia Riaz and Safeguarding lead is Jackie Harland.

Good Habits

E-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.
- Internet connection is provided via a service level agreement with BT Business, filtering is provided by the Draytex firewall and filter & is maintained by the ICT subject leader and technician employed by CPM Network Solutions.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;

- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

E-Safety Policy Communications

Introducing the E-Safety Policy to Pupils

- E-safety will be taught as part of the ICT curriculum and included as part of PSHE; this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet will be displayed and referred to around school.
- Pupils will be informed that networks and internet use will be monitored.

Staff and the E-Safety Policy

- All staff will be given the school's e-safety policy, will sign the Staff Acceptable Use Policy, and have its importance explained.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regards to these devices.
- They will be kept up to date of e-safety matters and of the current school e-safety policy and practices. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should ensure that lessons where internet is used are pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Enlisting Parent/Carer Support

- Parents/carers' attention will be drawn to the e-safety policy in newsletters and on the school website.
- They will be invited to parents' meetings to discuss e-safety and attend e-safety workshops and assemblies

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content is reported to the ICT technician who blocks the site from access within school
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

Pupil e-mail is currently unavailable within school. If a virtual learning environment is brought into school pupils will be provided with support on appropriate ways to use this system.

Social Networking

- Staff & pupils should not access social networking sites on school equipment without prior permission of the headteacher.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- 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.
- E-safety learning in school will tackle issues such as online grooming and sending inappropriate images and text messages (upper KS2).

Cyber-Bullying

The school regards cyber-bullying, through the inappropriate use of electronic communication such as text messages, email or postings on social networking websites like Facebook, as an unacceptable form of bullying. This includes the use of technology outside of school hours if it interferes with the safety and well-being of any member of the school community. Such incidents will be treated seriously, investigated thoroughly and appropriate disciplinary measures taken if necessary.

Filtering

The school works in partnership with, CPM Network Solutions & BT Business Draytex filtering solution to prevent access in inappropriate content.

Video Calls

- FaceTime and Skype are available to use in school. If used, this will be on a school account under the supervision of a teacher
- Pupils should ask permission from the supervising teacher before making or answering a video call.
- Video calls 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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required, or will use the teachers 2 parents' text messaging system.

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 head teacher 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.
- 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 the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority, CPM Network Solutions.

Protecting Personal Data

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

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 Rochdale Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the esafety policy is appropriate.

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 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Teaching Pupils to be safe online

Opportunities to teach pupils to be safe online will be both proactive and reactive. Proactive teaching will be planned for on medium term computing plans. Reactive teaching will occur where pupils ask questions or an incident arises, this will be noted on medium term planning as they arise.