Benton Dene Primary School E-Safety Policy

Written by Gemma Barber, September 2017

To be reviewed: September 2019

E-Safety Policy –

Introduction

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

This policy has been based on other primary schools' safety policies.

End to End 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 systems

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT and for child protection.

- E-Safety issues are included in the Child Protection, Health and Safety, Anti- Bullying, PSHEC and ICT policies.
- The e-Safety Policy will be reviewed January 2016

1.2 Teaching and learning

1.2.1 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.
- As Benton Dene Primary move towards 1-to-1 iPads for Key Stage 2 children, teaching children to access the internet responsibly and safely becomes an essential part of pupils' education.

1.2.3 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.

- 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 across the curriculum.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and details of content must be reported as soon as possible to the school ICT technician through the online reporting system.

- Staff 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.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.

- Virus protection will be installed and updated regularly.

- The school uses broadband with its firewall and filters.

1.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.

- 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 organisations 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.

1.3.3 Published content, the school web site and Twitter

- 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 will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully. We will only post photographs of those children whereby we have received photographic consent.

- Pupils' full names will not be used anywhere on the Web site or Twitter, particularly in association with photographs.

 Written permissions from parents or carers will be obtained on admission to Benton Dene Primary. These will be checked before photographs of pupils or pupils' work are published on the school Web site or the school's Twitter feed.

1.3.5 Social networking and personal publishing

 Social networking sites and 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. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

 Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

1.3.6 Managing filtering

 The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.

 If staff or pupils discover unsuitable sites, the URL, time and date must be reported via the ICT technician via online reporting system.

 Senior staff and the ICT technician will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 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 school time. The sending of abusive or inappropriate text messages is forbidden.

 Staff must ensure that all telephone communication with parents is

carried out through school telephones.

1.3.8 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Authorising Internet access

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

 All staff, including Teaching Assistants and Supply Teachers must read and sign the acceptable ICT Acceptable User Policy (AUP) before using any school ICT resource.

 Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

1.4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 will ensure that all procedures are carefully adhered to in the case that any unsuitable material is accessed.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with firstly by the class teacher, then by the ICT coordinators, the ICT technician or a senior member of staff.

Any complaint about staff misuse must be referred to a senior member of staff.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

All e-safety incidents will be reported by staff to the ICT technician via the online reporting system. The ICT coordinators or a senior member of staff will then deal with the incident according to the policies and procedures outlined in this document.

- Sanctions within the school discipline policy include: –

1. interview/counselling by class teacher / learning mentor
2. informing parents or carers
3. removal of Internet access or devise for a period of time

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

- Parents using school ICT equipment must sign an AUP consent form prior to use.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Pupils will be informed that Internet use will be monitored.

- Advice on e-Safety will be introduced at an age-appropriate level to

raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

1.5.3 Enlisting parents' / carers' support

Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters and via the website.