Benfieldside Primary School

E-Safety Policy

Policy and Practice
Implementation Date: December 2018
Review Date: December 2020
Reviewers: Mrs Addison – Headteacher, Mrs Lee ICT Lead
Adopted by the Governing Body – 2018/19

Benfieldside Primary School E-Safety Policy

At Benfieldside Primary School we see E-Safety as a core responsibility. The need to protect children from significant “external” risks on the Internet, and the need for direct teaching of responsible and safe ICT practices are vital aspects modern day education.

Writing and reviewing the E-Safety policy

The E-Safety Policy is part of the School Improvement Plan and directly relates to other policies including those for ICT and Safeguarding. The school has an appointed E-Safety Coordinator which is the Headteacher. The Headteacher is also the Designated Child Protection Officer, so the roles overlap.

Our E-Safety Policy has been written by the school, building on the Kent E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

Teaching and Learning

Why the Internet and digital communications are important.

The Internet is an essential element in 21st Century life for education, business and social interaction. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The school has a duty to provide pupils 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. 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 functions.

Internet use will enhance learning.

- The school’s Internet access will be designed to enhance and extend education.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, currently provided by ‘DurhamNet’ the County Approved Provider.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils have to sign a’ Pupils e-safety agreement’ at the start of each academic year. The rules are displayed in prominent positions all around the school.
- 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 shown how to publish and present information to a wider audience.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

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.

As pupils mature through our school, they will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught to report unpleasant Internet content (including images, text etc that make them feel uncomfortable) to the member of staff in charge of the group of children. This information will then be logged by the E-safety coordinator, and dealt with appropriately.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly by the school shared technician.

- Security strategies will be used as advised by the Local Authority, linking to Durhamnet Smoothwall Filtering and actual access to the school network.

Published content and the school website

- Staff or pupil personal contact information will not be published on the school website. The contact details given online should be the school office.

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

Storing and Publishing pupil's information, images and work

- All teaching staff will have access to an encrypted memory stick. This will be used in the event that staff need to store a pupil's information (short-term only) for use outside the school premises.

- Pupils' full names will not be used anywhere on a school Website or other online space, unless the express permission has been granted by the parents/carers of pupils via the Photographic Consent Form issued to parents/carers for completion when the child joins the school.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

- Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing

- The school will deny access to known social networking sites, and consider how to educate pupils in their safe use.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils will be educated regarding the risks linked to social network sites, in order to develop safe and responsible online behaviours.

- Parents will be given signposts to websites where they can gain information on supporting and reinforcing the e-safety messages promoted within school.

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

The school will work with Durham LA to ensure systems to protect pupils are reviewed and improved.
If staff or pupils come across unsuitable online materials, the site must be reported to the E-Safety Coordinator.
Staff may request website content to be unblocked for learning purposes only. Staff will do this by directly contacting the e-safety co-ordinator who will in turn contact ICT School Services to request this.
In advance of unblocked websites becoming 'live' on the filtering system, it is the responsibility of the member of staff who has made the request to check that the content is appropriate for use in school for teaching purposes.

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.
The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Children carrying mobile phones must hand their switched off devices to the office and they will be kept in the office to be collected at the end of the day by the child.

Policy Decisions

Authorising Internet Access

All staff within school must read and sign the Acceptable Use Policy before using any school ICT resource.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Handling E-Safety Complaints

- Complaints of Internet misuse by pupils will be dealt with by the Headteacher.
- 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. Mrs Addison (Headteacher) is our dedicated Child Protection Officer.

Communications Policy

Introducing the E-Safety policy to pupils

- Rules for Responsible Use of ICT will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- All staff have been given training in E-Safety by a Local Authority advisor. All staff also have had appropriate Safeguarding training.

- E-Safety education will be embedded within the ICT scheme of work. This will be a focused period of time each year and given a high profile.

Staff and the E-Safety Policy

- All staff will have access to the School E-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

- Staff will teach children how to safely search on the Internet and evaluate web based content.

Enlisting Parents and Carer Support

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website.

- The school will maintain a list of E-Safety websites for parents/carers.

Personal Data

Protecting personal data

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

Staff and Pupil Acceptable Usage Policies

The school operates both a Staff and Pupil Acceptable Usage Policy to ensure all members of the school community are aware of their personal responsibility in promoting e-safety for the benefit of all.

<u>Links To Other Policies</u>

This e-safety policy links to the following whole school policies outlined below:

- Data Protection Policy

- Child Protection and Safeguarding Policy