Drighlington Primary School e-safety Policy

Introduction

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband
- A school network that complies with the national standards and specifications.

E-Safety is the process of limiting risks to children and young people when using Information and Communication Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue which relates to the use of all ICT - fixed or mobile; current, emerging and future ICT.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our children and young people and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional and educational contexts. However alongside these benefits are potential risks that we have a statutory duty of care to manage, to ensure they do not become actual dangers to children and young people in our care or for employees.

At Drighlington Primary we have a policy in place which considers the following issues:

- the acceptable use of ICT by all users;
- e-safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incident when a user is at risk of or has come to actual harm through the use of ICT;
- e-safety training for staff and pupils
- the technology available to users, its security features and settings, e.g. virus protection, filtering and monitoring;

For Drighlington Primary School the named person with overall responsibility for e–safety is the Head Teacher.

The term ‘staff’ is used as a broad term within this policy and includes every adult who works on the school site, as well as volunteers and governors.

Drighlington Primary School’s e-Safety Policy will cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

E-Safety Risks & Issues
E-Safety risks and issues can be roughly classified into three areas: content, contact and commerce. The following are basic examples of the types of e-safety risks and issues that could fall under each category.

Content:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse

- Downloading of copyrighted materials, e.g. music and films
- Plagiarism

Contact:
- Grooming using ICT, leading to sexual assault and/or child prostitution
- Bullying using ICT (email, mobile phones, chat rooms etc)
- Children and young people self-publishing information - sometimes inappropriate - about themselves and therefore putting themselves at risk

Commerce:
- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Infrastructure Technology and Filtering
Firewall protection is provided for computers connected to the schools' network. It is the school's responsibility to ensure that anti-virus and anti-malware systems are installed and that the definition files are updated regularly on all school machines to maintain protection. If staff or pupils come across unsuitable on-line materials, the site must be reported to the Head teacher immediately.

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. 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.

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. 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 how to evaluate Internet content
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught to report unpleasant Internet content to adults.

Managing Internet Access

Information system security
School ICT systems security will be reviewed regularly. Virus protection will be updated regularly.

Internet Code of Conduct

- Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not permitted at Drighlington Primary.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise

materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.

- Virus infection and subsequent removal caused by such methods on machines without protection to the latest corporate standards will be the school's responsibility.
- To ensure compliance with the acceptable use policy for Web browsing and email the school reserves the right to monitor and record activity in these areas. All users should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

Email Code of Conduct

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send or publish their personal details in an email to an unknown recipient
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.

Published content and the School Website Code of Conduct

Staff or pupil personal contact information will not generally be published. 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.

- Only designated staff member(s) within the school may authorise the uploading of material to the school website.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes, i.e. school web site will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Home addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.

Publishing Pupils' Images and Work Code of Conduct

- Photographs that include pupils will be selected carefully so that their image cannot be misused.
- Written permission from parents or carers will be obtained before photographs of pupils that may include their full names, are published on the school Website.
- Staff should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Protecting Personal Data

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

Staff and the e-safety policy

- All staff will be given 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 always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' 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.
- The school will ask all parents to sign consent forms.
- The website will give e-safety guidance for parents and carers.

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.

Reviewed 10.11.21

Next review July 2024