Ladywood Primary School

E-Safety Policy January 2023

Ladywood Primary School

E-Safety Policy

At Ladywood Primary School we are committed to the safe-guarding and well-being of every child in school. This policy outlines the main aspects of our safety guidelines and procedures when using electronic learning. (E-learning)

Introduction

This guidance document provides advice on appropriate and safer behaviours with technology for adults working in paid or unpaid capacities, in school or elsewhere. It is intended to be used to ensure safe usage of ICT and electronic technology by all and to make staff aware of both potential dangers and appropriate and professional behaviour.

The Internet has become an integral part of children's lives, enabling them to undertake research for school projects, talk to their friends and access information from around the world. Increasing provision of the Internet in and out of schools brings with it the need to ensure that learners are safe.

This policy sets out the aims to achieve this.

The School Aims

- Children should always be supervised by a responsible adult when using the Internet.
- Teachers should evaluate any websites fully before they use them with their students. Often this means checking the websites, search results etc before the lesson.
- What may be considered a safe site today might not be tomorrow. Pay particular attention to image advertisements as they can change each time the web page is accessed.

Effective Practice in e-Safety

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 from an approved Network;
- A school network that complies with the National Education Network standards and specifications.

Teaching and Learning

- Internet and digital communications are important because 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.
- 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 how to report unpleasant Internet content

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and our dedicated Code Green technician, John Greenhaugh

E-mail

- 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.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff emails will be shared with parents on our website to enable them to communicate with class teachers, should they need to.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- During occasions whereby the school is forced to close, staff emails will be shared on the website to allow parents to contact staff regarding work set.
- Class teachers will be responsible for updating their own class page. It is essential that teachers know which children have written permission for the website. This can be found on SIMS.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that the image cannot be misused.
- Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

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

- 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, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be advised not to communicate with parents and pupils using social network site.
- Staff are reminded that discussing school matters on social network sites is a breach of confidentiality and thus a breach of their terms and conditions of employment.

Managing filtering

- The school will work with the Network provider and Code Green to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the senior leadership team and the Code Green technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- Mobile phones are not allowed in school. If children do need them they are kept in the school safe until home time and then handed back to the pupil. The phone will be turned off during the day. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR May 2018.

Authorising Internet access

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

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. Neither the school nor Barnsley LA can accept liability for any 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 e-safety policy is appropriate and effective.

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 headteacher.
- 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 (see schools complaints policy)

- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly as part of the ICT curriculum.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety is covered in classes throughout school.
- E-Safety training will be embedded within the curriculum schemes of work and in the PD curriculum.

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 that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Policy reviewed by J Lassu January 2023

APPENDIX A - Useful Websites

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Kidsmart
www.kidsmart.org.uk/