

**Hollin Primary School**  
**e-Safety Policy**

September 2018



# Contents

Introduction.....	
- Why does a school need an e-safety policy? .....	2
Teaching and Learning.....	
- Why internet and digit communications are important.....	3
- Internet will enhance learning.....	3
- Pupils will be taught how to evaluate Internet content.....	3
Managing Internet Access.....	
-Internet System Security.....	4
-Email.....	4
-Published content and the school website.....	4
-Publishing pupil's images and work.....	4
-Managing social networking, social media and personal publishing.....	4
-Managing filtering.....	5
-Managing emerging technologies.....	5
-Protecting personal data.....	6
Policy Decisions.....	
-Authorising Internet access.....	7
-Assessing risks.....	7
-Handling e-safety complaints.....	7
-Community use of the Internet.....	7
Communications Policy.....	
-Introducing the e-safety policy to pupils.....	7
-Staff and the e-safety policy.....	8
-Enlisting parents' support.....	8

# Introduction

## Why does a school or setting need an e-safety policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection. This policy document sets out the school's aims, principles and strategies for using the internet and protecting pupils.

At Hollin Primary School:

- Our e-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised September 2018
- It was approved by the Governors September 2018

# Teaching and learning

## **Why 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 our children 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 allows rapid progress in acquiring knowledge.
- Internet access supports and enriches teaching and learning on a daily basis.

## **Internet use will enhance learning**

- The school Internet access is provided by through a EDIT contract and includes content 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 appropriately to a wider audience using suitable software.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

## **Pupils will be taught how to evaluate Internet content**

- The school will seek to 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.
- Pupils will be taught how to report unpleasant Internet content and what constitutes such content.

# Managing Internet Access

## Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- The use of user logins and passwords to access the school network will be enforced.
- Security strategies will be discussed with EDIT

## E-mail

- Pupils may only use approved e-mail accounts on the school system on Purple Mash
- 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.
- Staff to pupil email communication must only take place via a school email address or from within a learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

## 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 IT technician will take overall editorial responsibility for online content published by the school, and ensure that content is accurate and appropriate.

## Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and be published on the school website without mention of the child's name. Additionally, the school will seek parental permission before any photos of children are published on the school website.
- Pupils' full names will not be used on the Website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

## Managing social networking, social media and personal publishing

- The school will control, and block where possible, access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils must not place personal photos on any social network space provided on a learning platform.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- 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 on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be advised to use nicknames and avatars if using social networking sites.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

### **Managing filtering**

- The school will work in partnership with EDIT 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 e-Safety Coordinator.
- EDIT 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.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with pupils is required.

### **Protecting personal data**

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

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

## Policy Decisions

### Authorising Internet access

- All staff must read and sign the 'Staff AUP for ICT ' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- **At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.**
- **At KS2 pupils must understand, read and sign for Internet access individually by agreeing to comply with the 12 Rules for Acceptable Use.**
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

### 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 LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will 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.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

### **Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

## **Communications Policy**

### **Introducing the e-safety policy to pupils**

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils

### **Staff and the e-Safety policy**

- All staff will be given access to the School e-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage and monitor ICT use will have clear procedures for reporting issues to the IT Technician or ICT co-ordinator.

### **Enlisting parents' 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.
- Parents and carers will from time to time be provided with additional information on e-safety.