

**ELLESMERE  
PRIMARY SCHOOL**



Engage, Persevere, Succeed

**E- Safety Policy 2017-2018**

Review Date: December 2017

## **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.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations.

### **Internet use will enhance learning**

The school Internet access will be designed expressly for pupil use and will include LA filtering appropriate to the age of pupils.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear directives 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 taught how to evaluate Internet content**

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught about the importance of 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 to a member of staff. Staff will then record this on a concerns form from the e-safety folder kept by the e-safety co-ordinator.

## **Managing Internet Access**

### **Information system security**

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be in line with Local Authority guidelines.

## **E-mail**

Pupils will only use the class Office 365 e-mail accounts which can be monitored by the class teacher to ensure that due consideration is given to how e-mail from pupils to external bodies is presented and controlled.

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.

## **Published content and the school web site**

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

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## **Social networking and personal publishing**

The authority filters block access to social networking sites.

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 off school premises.

## **Managing filtering**

Shropshire Council will 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 and headteacher.

The authority 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 as appropriate.

Mobile phones will not be used in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The appropriate use of Learning Platforms will be discussed as the children are introduced to the use of the technology.

Staff should use the school phone where contact with pupils is required.

## **Protecting personal data**

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

## **Policy Decisions**

### **Authorising Internet Access**

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.

Staff pupils and parents will be required to sign an acceptable use policy/consent form detailing the proper use of technologies in or associated with the school including the learning platform.

## **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 the local authority can accept liability for any material accessed, or any consequences of Internet access.

The school will review ICT use along with the e-safety policy to establish if the policy is adequate and that the implementation of the 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 head teacher.

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.

Sanctions include:

For misuse of the learning platform - child concerned will have their access to the learning platform blocked.

For misuse of the internet in school - consequences will be in line with the school behaviour policy and may include controlled access to technology in school if deemed necessary by the class teacher.

## **Communications Policy**

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

e-Safety rules will be discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

All pupils will be made aware of the importance of e-safety and this subject will be revisited yearly.

e-Safety training will be embedded within the ICT scheme of work and will be discussed at the beginning of each new school year.

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

All staff and governors will be issued with the School e-Safety Policy and its importance discussed.

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.

### **Enlisting parents' and carers' support**

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

The school will ensure that parents have access to suggestions for safe home Internet use.

## Reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Bullying and Child Protection.

The school has appointed an e-Safety Coordinator. This will be part of the ICT co-ordinator role as the responsibilities overlap

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

### Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use the Office 365 class e-mail accounts. Pupils should never give out personal information.	Office 365