

## **Redby Primary School**

### **E-safety policy**

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Child Protection, Curriculum, Data Protection and Security.

E-Safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- safe and secure broadband including the effective management of filtering.
- the appointment of an e-Safety Coordinator to implement and monitor this policy.

#### **1. Introduction**

The purpose of this policy is to:

- establish the ground rules we have in Redby Primary School for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- describe how these fit into the wider context of our discipline and PSHME policies.
- demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

#### **2. Teaching and learning**

- the Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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 Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- the school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

### **3. Managing Internet Access**

- school ICT systems capacity and security is reviewed regularly.
- virus protection is updated regularly.

#### **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.
- pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- e-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.

#### **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 is not published.
- the headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified.
- pupils' full names are not used anywhere on the Web site,.
- written permission from parents or carers must be obtained before photographs of pupils are published on the school Web site.
- pupil's work will only be published with the permission of the pupil and parents.

#### **Social networking and personal publishing**

- the school blocks access to social networking sites.
- newsgroups are also blocked.
- pupils are told never to give out personal details of any kind which may identify them
- pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

#### **Managing filtering**

- if staff or pupils discover an unsuitable site, it must be reported immediately to the e-Safety Coordinator.
- senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.

#### **Managing videoconferencing**

- videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
- pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- videoconferencing is appropriately supervised for the pupils' age.

### **Managing emerging technologies**

- emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- mobile phones are not used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

### **Protecting personal data**

- personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **4. Policy decisions**

### **Authorising Internet access**

- all staff read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- the school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access be withdrawn.
- at Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- at Key Stage 2, access to the Internet will be by supervised access to specific, approved on-line materials.
- parents are asked to sign and return a consent form.

### **Assessing risks**

- the school takes all reasonable precautions to ensure that users access only appropriate material by using Sunderland's filtering system.
- the school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

### **Handling e-safety complaints**

- complaints of Internet misuse are dealt with by a senior member of staff.
- any complaint about staff misuse are referred to the headteacher.
- complaints of a child protection nature are dealt with in accordance with the school's child protection procedures.
- pupils and parents are informed of the complaints procedure.

## **5. Communications**

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

- e-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year.
- pupils are informed that network and Internet use will be monitored.
- as part of the Every child matters agenda, Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre: [thinkuknow.co.uk](http://thinkuknow.co.uk)

**Staff and the e-Safety policy**

- all staff have copies of the school's e-Safety Policy and know its importance.
- staff are aware that Internet traffic can be monitored and traced to the individual user.

**Enlisting parents' support**

- parents' attention is drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school Web site.

This policy will be review annually by the governors and staff.

E-safety policy  
February 2007

Mrs Pauc  
Subject Leader

## Redby Primary School

### Rules for Responsible Internet Use

**The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.**

- I will only access the system with my own login and password, which I will keep secret;
- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will not bring any portable data storage into school;
- I will ask permission from a member of staff before using the Internet;
- I will not download program files from the Internet.
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not give my home address or telephone number, or arrange to meet someone;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

## Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of ICT skills, Redby Primary School is providing supervised access to the Internet including e-mail and video conferencing.

Our school Internet access provider operates a filtering system that restricts access to inappropriate materials and video conferencing uses the educational broadband network to ensure quality of service and security.

The access your child will have to the Internet will be highly planned for and appropriate to enhance their educational needs. I enclose a copy of the Rules for Responsible Internet Use that we operate at Redby.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Mrs V Shield

Headteacher

---

### **Permission for Internet Access**

#### **Parent/carers permission**

I give permission for access to the Internet on the terms set out in the above letter.

Signed: \_\_\_\_\_

Print name: \_\_\_\_\_

Date: \_\_\_\_\_

#### **Pupil's agreement**

I agree to follow the rules for Responsible Internet Use.

Signed: \_\_\_\_\_

Print name: \_\_\_\_\_

Class: \_\_\_\_\_