E-Safety Policy

September 2017

Robert Peel Primary Schools Online Safety Policy outlines what we will to safeguard children using the internet. The policy has been drawn up through the involvement of the whole school community and we are committed to developing an e-safety culture whereby children are able to use the internet in a safe and effective way. Our school vision encompasses our passion to ensure children are able to succeed in a safe environment.

At Robert Peel Primary School our vision is to develop confident, resilient and independent learners who are able to communicate effectively with others. Our aim is for the children to be happy in all aspects of school life and for them to aspire to be the best they can be.

We will achieve this by creating a culture of independent learning and discovery that is stimulating and enjoyable for both children and staff. The children's views will be sought and valued and high expectations will ensure that all children achieve even when challenged.

Introduction

The school has a Designated e-Safety Leader (M James), who is also one of the Designated Safeguarding Leads, as the roles overlap. He works in collaboration with the Subject Leader in ICT ensure this policy meets the ever-changing issues relating to the Internet and its safe use.

The e-safety policy forms part of the schools safeguarding procedures and relates to other policies including those for ICT, bullying and for safeguarding and child protection.

Our e-safety Policy has been written by the school, building on government guidance. It has been agreed by staff and approved by governors. The e-safety Policy and its implementation will be reviewed annually

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide 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 will enhance learning.

The school's 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 taught how to evaluate internet content.

We will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

As pupils progress through the school into Key Stage 2 they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Children will be educated in the 'Think then Click' check list.

Information System Security

School ICT systems capacity and security will be reviewed regularly.

Virus and Spyware protection will be installed and updated regularly.

Security strategies will be discussed with the Local Authority and with the ICT technician.

Email

Pupils may only use approved e-mail accounts, e.g. It's Learning VLE email.

Pupils must immediately tell a teacher if they receive offensive e-mails.

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 should be written carefully and authorised by a teacher before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Email subscriptions to websites or other electronic services should be authorised.

Published Content and the School Website

The contact details on the school's web site include the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Deputy Head will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images, Videos and Work

Photographs and videos that include pupils will be selected carefully. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils' full names will not be used in association with photographs or videos.

Written permission from parents or carers will be obtained before photographs and videos of pupils are published on the school's web site.

Work can only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing

The school will block / filter access to inappropriate social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Social Media Site and Youtube are not accessible through the school network to children in school.

Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Staff must not communicate with children using public social networking sites such as Facebook, MySpace, Twitter, etc.

Any Virtual Learning Environment (VLE) the school chooses to use may be used to communicate electronically with children.

Staff should not communicate with parents about school-based issues using public social networking sites such as Facebook, MySpace, Twitter, etc.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.

Managing Filtering

The school will work in partnership with the LA and E-Safety Group to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Lead and ICT Technician.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting Personal Data

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

Authorising Internet Access

All staff must read and follow the 'Staff Code of Conduct' set out in the staff handbook 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.

Parents will be asked to sign and return a consent form for Internet and Acceptable ICT Use Agreement.

Staff laptops and email are password protected.

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. The school will audit ICT use to establish if the e-safety effectively and continue to work with parents and carers about teaching their children to be safe online.

Handling e-safety Complaints

Complaints of internet misuse will be dealt with by the Headteacher or next senior member of staff on site.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

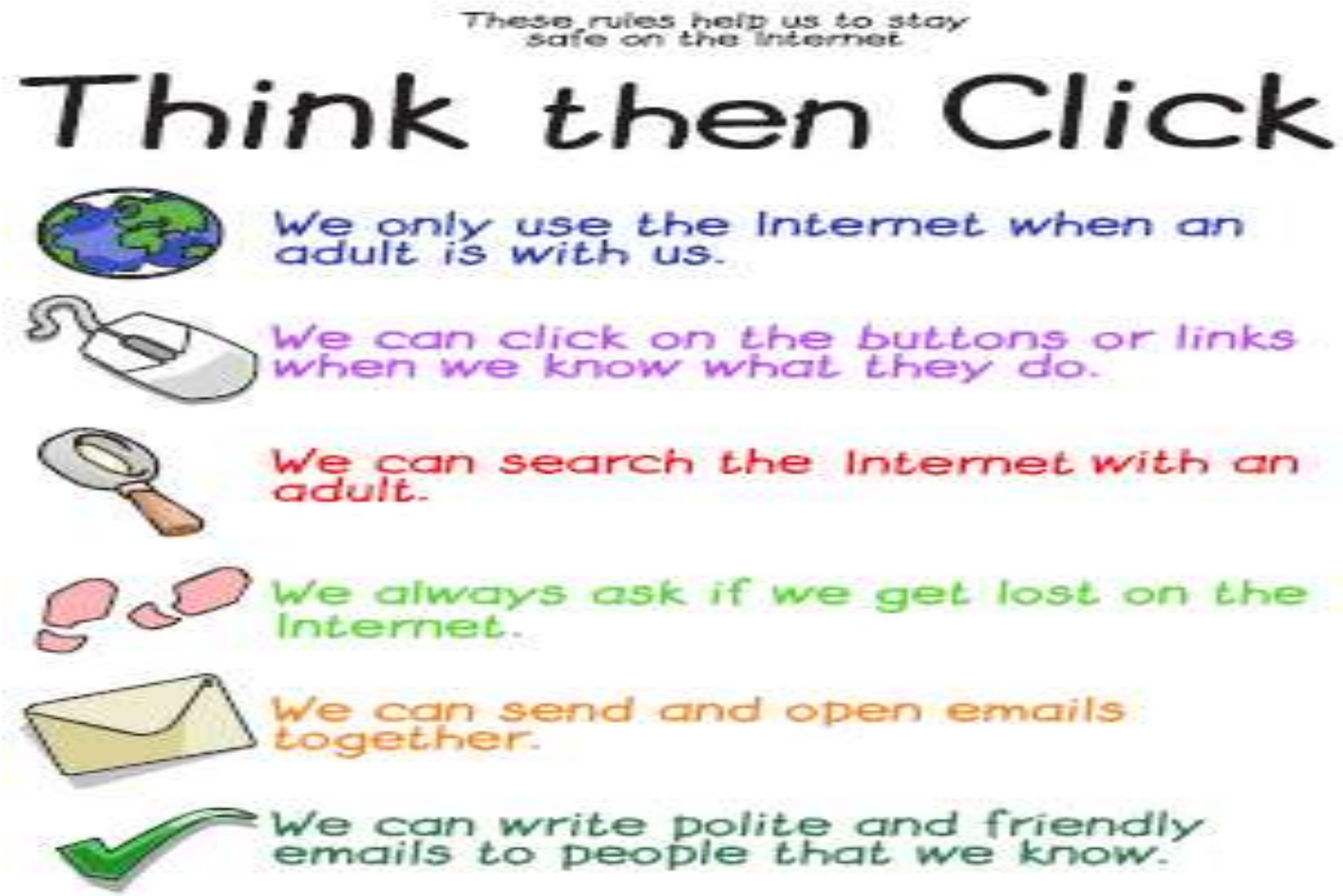
Pupils and parents will be informed of the complaints procedure if required.

If required external advice will be sought from the LA.

Introducing the e-safety Policy to Pupils

E-safety rules 'Think then Click' will be posted in all classrooms where computers are used.

Users will be informed that network and internet use will be monitored.



Staff and the e-safety Policy

All staff will be given a copy of the school's 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 who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting Parents' Support

Parents' attention will be drawn to the school's e-safety policy in newsletters, the school brochure and on the school website.

Parents will be informed about the Think the Click rules taught to the children in school and will be informed that they may wish to invest in security software for their own computers.

Parents to be signposted to useful sites to help keep their children safe at home.

https://www.thinkuknow.co.uk/

http://www.childnet.com/parents-and-carers

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

.