Lemington Riverside E-safety Policy

Teaching and Learning

Why is Internet use important?

The purpose of Internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for all pupils. Our school has a duty to provide pupils with quality Internet access.

The ICT coordinator will be responsible for e-safety on a day to day basis.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering by the LA.

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

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

As appropriate, pupils will be taught the importance of cross checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. using CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information system security

School ICT systems security is regularly reviewed and training has been delivered by the LA to children, staff, governors and parents.

Virus protection is updated regularly.

Security strategies are discussed with the LA.

E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive, inappropriate or upsetting e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, 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 will monitor e mails from pupils to external bodies.

The forwarding of chain letters is not permitted.

Published content and the school Website

Staff or pupils' personal information will not be published.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

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

Publishing pupil's images and work

Pupils' full names will not be used anywhere on the School Web site without parental permission, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Pupil's work will be published with the permission of the pupil.
Parents will 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 educate pupils in the safe use of social networking sites.
Newsgroups are not accessed by pupils at school.

Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils are advised to use appropriate nicknames and avatars when using social networking sites.

Managing filtering

The school will work in partnership with the LA to ensure filtering systems are as effective as possible.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator, who will take the appropriate action.

Managing video conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and web cam use will be appropriately supervised for the pupils' age.

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 are aware 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 will not be used during lessons or formal school time. If children bring mobile phones into school then they will be kept in the office until home time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Staff will be issued with a 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

All staff must read and sign the 'Staff Code of Conduct 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 Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials.

Parents will be asked to sign and return a consent form giving their children permission to use the internet under supervision.
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 ensure that users access only appropriate 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 school computer. The school can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective and appropriate.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the e-Safety Co-ordinator in the first instance .

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.

Parents and pupils will need to work in partnership with staff to resolve issues are informed of the complaints procedure

Pupils and parents will be informed of the consequences for pupils misusing the Internet.
Discussions will be held with the LEA to establish procedures for handling potentially illegal issues.

.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules are posted in all networked rooms with Internet access and discussed with the pupils regularly

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

A programme of training in e-Safety is in place based on the materials from CEOP.

Staff and the e-safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff are informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always use a search engine filtered by the LA when accessing the web with pupils.

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.

The school will maintain a set of e safety resources for parents/carers.

The school will ask all new parents to sign the Internet Access permission form when they register their child with the school.

Internet issues will be handled sensitively, and parents will be advised accordingly.

To be reviewed on an annual basis

Policy discussed amended and agreed at Staff Meeting 5.10.10

Approved by the Personnel Committee on 7.2.11

Reviewed in December 2013

Reviewed in December 2014

Reviewed : 11. 1.16

Reviewed : 30.11.16

Reviewed: 13.11.17

Reviewed: 12.11.18
Date to be reviewed : November 2019