Review Cycle	Annually
SLT member responsible	JM
Committee	Curriculum
Date adopted	25 02 2015
Review Date	February 2016

LITCHAM SCHOOL
E-SAFETY POLICY

Writing and reviewing the e-Safety policy

The e-Safety & Acceptable Use Policy is part of the School Development Plan and relates to other policies including those for ICT, anti-bullying and for child protection.

The Head of Student Support has an overview of e-Safety, (Senior Designated Professional).

Our E-Safety & Acceptable Use Policy has been written by the School, building on best practice and government guidance. It has been agreed by the Leadership Team and approved by Governors.

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 students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and students.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Students will be educated in the effective use of the Internet

Students will be shown how to publish and present information appropriately to a wider audience.

Students 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 students complies with copyright law.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Students will be taught how to report unpleasant Internet content e.g. using the Child Exploitation and Online Protection Centre (CEOP) Report Abuse icon or 'Report Bullying' button on the School website.

Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies may be discussed with the Local Authority.

E-mail

Students and staff may only use approved e-mail accounts on the school system.

Students must immediately tell a teacher if they receive offensive e-mail.

Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Staff to student e-mail communication must only take place via a school e-mail address, or from within the 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 students to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the website will be the school address, e-mail and telephone number.

Certain members of staff's named school e-mail address will be given. Staff or students' personal information will not be published.

The Network Manager will take overall editorial responsibility and ensure that content is accurate and appropriate. Oversight is given by the Leadership Team and the link governor.

Publishing photographs, images and work

Photographs that include students will be selected carefully and parental permission is gained for all photographed students.

Written permission from parents or carers will be obtained before photographs or images of students are published.

Written permission from adults will be obtained before their names, photographs or images of themselves are published.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

The School will control access to social networking sites on its network and consider how to educate students in their safe use, e.g. use of passwords.

Newsgroups will be blocked unless a specific use is approved.

All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

Students must not place personal, non-school related photos on any social network space provided in the school learning platform without permission.

Students, parents and staff will be advised on the safe use of social network spaces on our website.

Managing filtering

The School will work in partnership with Norfolk Children's Services to ensure systems to protect students are reviewed and improved.

If staff or students come across unsuitable on-line materials, the site must be reported to the nominated member of staff.

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

Managing videoconferencing

Videoconferencing will use the School's chosen broadband provider to ensure quality of service and security rather than the Internet.

Students should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the students' 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.

Other devices

Mobile phones are NOT permitted to be used within the classroom, unless specifically authorised by the teacher.

Filming and photographing educational activities must be undertaken using school equipment.

Taking photographs at any time without the subject's consent is not permitted.

The sending of abusive, offensive or inappropriate material is forbidden by law.

Staff must not share personal telephone numbers with students and parents. (A school phone will be provided for staff where contact with students 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 students who are granted access to School's ICT systems.

Parents will be asked to sign and return a consent form.

Students must agree to comply with the Responsible Internet Use statement before being granted Internet access.

Any person not directly employed by the School will be asked to sign the Staff, Governor and Visitor e-Safety & ICT Acceptable Use Agreement before being allowed to access the Internet on 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 Norfolk Children's Services, 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 referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school safeguarding and child protection procedures.

Students and parents will be informed of the complaints procedure.

Students and parents will be informed of consequences for students misusing the Internet.

Community use of the Internet

All use of the School's Internet connection by community and other organisations shall be in accordance with the School's E-Safety policy.

Communications

Staff and the e-Safety policy

All staff will be given access to the Staff, Governor and Visitor E-Safety & ICT Acceptable Use Policy. Its importance will be explained and they are expected to sign in agreement.

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.

Introducing the e-Safety policy to students

Appropriate elements of the E-Safety policy will be shared with students.

E-Safety rules will be posted in all networked rooms.

Students 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 students.

All students must comply with *e-Safety and Acceptable ICT Use Rules for Students.*

Enlisting parents' support

Parents' and carers' attention will be drawn to the School's E-Safety & Acceptable Use Policy, for example in newsletters, the school brochure and on the school website.

Parents and carers will from time to time be provided with additional information on E-Safety.

The School will ask all new parents to sign the E-Safety & ICT Acceptable Use Agreement for Parents/Carers when they register their child with the School

Signed: Dated:

Chair of full governing body