LONGBENTON
HIGH SCHOOL

E-Safety Policy

RESPONSIBILITY:	Headteacher
IMPACT ASSESSMENT:	Yes
GOVERNING COMMITTEE:	Finance & Premises Sub-Committee
REVIEWED:	May 2012
RATIFIED:	May 2012
WEBSITE:	Yes

E-safety

E-safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. 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.

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

End to End E-safety

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 from North Tyneside LA and effective management of the web filtering.
- National Education Network standards and specifications.

Further Information

Mr I Williams, E-safety Co-ordinator	iw@lblearning.com
North Tyneside IT helpdesk	0191 643 5444
North Tyneside E-safety	www.esafetynorthtyneside.org.uk
Becta E-safety	www.becta.org.uk/schools/esafety

Teaching and learning

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 students and staff with quality Internet access as part of their learning experience and professional development.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school Internet access will be designed expressly for student use and will include filtering to prevent students from accessing inappropriate material.
- Students will be aware of issues of copyright and intellectual property.

Students will be taught how to evaluate Internet content

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- School staff should try to ensure that the use of Internet derived materials by staff and by students complies with copyright law.

Managing Internet Access

Information system security

- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Students must immediately tell a teacher if they receive offensive or inappropriate e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Headteacher or E-safety Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs on the external website, that include students, will be selected carefully and will not be published without the prior permission of parents/carers.
- Students' full names will not be used anywhere on any external website in association with photographs without the written permission of parents or carers.
- Work can only be published with the written permission of the student and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.

- Students and staff must not place personal photos on any social network space without the permission of the person involved.
- Students and staff must not make comments about members of the school without their permission on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and taught how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The school will work in partnership with the LA to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff 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 and a risk assessment will be carried out before use in school is allowed.
- Except when directed by staff, mobile phones and other ICT related equipment will not be used during lessons, assemblies, detentions or meetings.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff contact with parents and students should be via school telephones.

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, students and governors who are granted access to school ICT systems.
- Students, staff and governors must comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form.

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 the LA 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.

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 dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police when handling potentially illegal issues.

Community use of the Internet

- The school requires community users to comply with the school e-safety policy.

Communications Policy

Introducing the e-safety policy to students

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.

Staff and the E-safety policy

- All staff will be given the School 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 that 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 E-safety Policy in newsletters, the school brochure and on the school website.

Violating the Acceptable Use Policy

Any conduct which violates the Acceptable Use Policy or any other conduct which is deemed unsuitable will contravene the conditions, and may result in any or all of the following:

- BFL sanctions – C3, C4, C5.
- Restricted network access.
- Loss of network privileges.
- Disciplinary or legal action including criminal prosecution under appropriate laws.