LONGBENTON
HIGH SCHOOL

E-Safety Policy

RESPONSIBILITY:	**Headteacher**
IMPACT ASSESSMENT:	**Yes**
GOVERNING COMMITTEE:	**Finance & Premises Sub-Committee**
REVIEWED:	**May 2017**
RATIFIED:	**June 2017**
WEBSITE:	**Yes**

INTRODUCTION

The curriculum requires students to learn how to locate, retrieve and exchange information using ICT. Teachers need to plan to integrate the use of communications technology such as web-based resources and email. ICT skills are vital to access life-long learning and employment.
Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings students into contact with a wide variety of influences, some of which may be unsuitable. Unmediated Internet access through computers, telephones, Ipads etc. brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Safeguarding Policy, including Preventing Radicalisation/Extremism

CORE PRINCIPLES

- Guided Educational Use – curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk Assessment – students must be protected from danger (violence, racism, exploitation) and learn how to recognise and avoid it.
- Responsibility – all staff, governors, external providers, parents and students must take responsibility for the use of the Internet.
- Regulation – in some cases eg. unmoderated chat rooms, immediate dangers are presented and their use is banned. In most cases strategies on access must be selected and developed to suit the educational activities and their effectiveness monitored.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband and effective management of the web filtering.
- National Education Network standards and specifications.
- This policy is closely related to the guidance contained in; Keeping Children Safe In Education – statutory guidance to schools and colleges (DfE July 2015).
- With regard to Radicalisation via the internet and social media the school fully adopts The Prevent Duty – departmental advice for schools and childcare providers (DfE June 2015) – see Longbenton High School's Safeguarding and Child Protection Policy.

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

Importance / Benefits of Internet Use

- Raise educational standards, promote pupil achievement.
- Support work of staff and enhance management systems.
- Part of the curriculum and a necessary tool in teaching and learning.
- Students are entitled to quality Internet access as part of their 21st century learning experience.
- Access to worldwide resources and experts.
- Educational and cultural exchanges between students worldwide.
- Facilitate staff professional development.
- Communication with external services.
- Exchange of curriculum and administrative data/sharing of good practice.

Ensuring That Internet Use Enhances Learning

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Internet access will be designed expressly for student use and will include filtering appropriate to students' ages.
- Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet.
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age.

Student Evaluation of Internet Content

- Any user discovering unsuitable sites must report the address and content to; the Internet Service Provider, the Network Manager, a teacher or the Designated Child Protection Co-ordinator as appropriate.
- Students will 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 to acknowledge the source of information and to respect copyright when using Internet material in their own work.

MANAGING INTERNET ACCESS

ICT System Security

- The school's ICT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly.
- Files held on the school's network will be regularly checked.
- Use of portable media such as USB connected memory sticks or drives.
- Security strategies will be discussed with the Local Authority and other advisors.
- Downloading of unauthorised files will be prohibited, and where possible blocked.
- Use of the school's ICT systems will be subject to the Data Protection Act and the Computer Misuse Act.

Management of Email

- Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.
- Pupils may only use approved email accounts on the school system.
- Pupils must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication.
- Social email can interfere with learning and will be restricted.
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending.

Management of the Content of the School Website

- The point of contact on the website should be the school address, email and telephone number. Staff and students' home information will not be published.
- The Network Manager, acting as the Headteacher's nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate, working alongside the school's SLT.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

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 permission of parents or carers.
- Work can only be published with the permission of the student and parents.

Social Networking

- The school will block/filter access to social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students will not be allowed access to public or unregulated chat rooms, social networking sites and forums.
- Students may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised.
- YouTube access is a medium that has benefits which include helping teach pupils how to use the internet appropriately and safely, and how to conduct online research effectively. Across our network we ensure YouTube is set to 'restricted mode' before allowing pupils to use it. This is a setting on YouTube that blocks content intended for adult users only.

This is to minimise the risk that they will see something inappropriate, whether deliberately or by accident, or will waste lesson time viewing non-educational content.

Management of Filtering

- The school will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the Designated Teacher i/c Child Protection if necessary) immediately.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time.

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

Authorisation of Internet Access

- The school will maintain an up to date record of all staff and students who are granted Internet access.
- Internet access will only be given to authorised devices. This will be managed by the Network Manager.
- All Internet access is monitored and recorded using electronic means.
- All staff and students (and students' parents) must sign the Acceptable Use Policy.

Risk Assessment

- Some material available via the Internet is unsuitable for students. 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 use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risk will be reviewed regularly.

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

COMMUNICATIONS POLICY

Student, Staff and Parental Awareness
- All stakeholders will be made aware of this policy and how it relates to them.
- All staff will sign the Acceptable Use Policy.
- 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.
- All students will sign the Acceptable Use Policy – countersigned by parents.
- Students will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the PSD/RSD and Computer Studies programmes, covering use in school and outside of school.
- The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by the Network Manager and responsible Assistant Headteacher as well as the Director of Support Services.
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required.
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available.
- Cases of internet misuse and other disciplinary breaches related to the

policy will be dealt with through the school's Behaviour, Bullying and Safeguarding/Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery. Board and the Channel Panel (after consultation with KSCB and Police)

- Any complaints associated with the application of this policy will be dealt with through the school's Complaints Procedure.

Violating the E-Safety 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.

Review of policy

The Governing Body of Longbenton High School have agreed to review this policy annually as it is an area of constant change.