



Beacon Hill School
E Safety Policy.
1.11.

The E-Safety Policy helps us deliver the aims of Beacon Hill School in the following ways:

1. That has high expectations for continuous improvement in order to raise standards for pupils.

The E-Safety Policy introduces safer guidelines for the implementation of new ICT software and applications. This will enable the students to access and take advantage of these to further develop their digital and ICT skills.

2. In which all partners include, involve and inform each other.

The E-Safety Policy will lay down specific networks of communication between partners to ensure those who need to be informed of issues and areas of concern are so. It also specifies the direct movement of information from student to LEA ICT Advisor. This should help the whole LEA with Internet/Digital dangers.

3. That actively develops parental partnerships for the benefits of the pupils.

The E-Safety Policy will create opportunities for the development of parental partnerships through the passing of information and the further education of parents about the dangers surrounding the Internet and digital devices. In tandem, it will also lay the ground work for highlighting the advantages and implementations of the fast moving world of ICT. This will enable the parents to make more informed decisions linked to their children and their uses of ICT in both school and at home.

4. That positively promotes and encourages independence, confidence and self advocacy.

The E-Safety Policy will provide both Students and Staff with a clear set of guidelines linked their use of ICT. This should enable them to make better informed decisions concerning how it is used in the classroom and out in the community. As a result both groups should be more confident in their independent use of a wider range of digital and ICT based resources.

5. That values communication and provides the time and opportunity to make it effective.

The E-Safety Policy positively endorses the new digital means of mass communication. It encourages their use by both staff and students and aims to ensure this is done as safely as possible.

6. That extends inclusion within the school and beyond.

The E-Safety Policy will support the further use of ICT within the school by both Students and Staff. More specifically, it will encourage the use of a wider range of communication and information sharing devices, software and formats. This will extend the sharing of information, between our students and staff and our mainstream peers and partners.

7. That gives pupils the skills and opportunities to make informed choices.

The E-Safety Policy will enable staff to support the students in developing their own awareness of the advantages and benefits of using ICT as well as the possible dangers.

8. That establishes an atmosphere of security, trust and respect for all.

This is at the heart of the E-Safety Policy. Fundamental to its implementation is the aim of creating a safe environment for all ICT users in the school community. It will also lay down the expectations of conduct for all users and the means of dealing with any inappropriate use. It stresses the need for greater awareness of the safety issues surrounding a greater use of digital and Internet resources in school and the wider community.

9. That celebrates achievement for all.

The E-Safety Policy will create a more appropriate environment for students to share their work and achievements through a wider range of mediums and with a larger group of peers and audiences.

E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children.

Schools need to protect students and staff but also to protect themselves from legal challenge. However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken to protect users.

A very present danger

Despite precautions at school, open access to the Internet has become an integral part of children's lives. A growing danger is presented by the ease of uploading material to the web.

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 both in administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the LA including effective management of web filtering.

Learning and Teaching

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 with quality Internet access as part of their learning experience.

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

Internet use will enhance learning

- The school Internet access will be designed expressively for student use and will include appropriate filtering.
- 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 in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Schools should 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E-mail

- Students may only use approved e-mail accounts on the school system.
- Students must immediately inform an adult if they receive an 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.
- E-mail sent to an external organization should be written carefully and authorized before sending, in the same way as a letter written on school headed paper.
- Only Gmail may be used by staff on school lap tops, (inc. lap tops provided for teachers).

Published content and the school web site

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The Senior Management Team will take overall responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Further written permission from parents or carers will be obtained before photographs of pupils are used for any purpose on a public accessible web site.
- No full names will ever be used with photographs.

Social networking and personal publishing

- 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 should be advised on security, deny access to unknown individuals and how to block unwanted communications if using social networking sites at home.

Managing filtering

- The school will work in partnership with the LA to ensure systems to protect pupils are reviewed and improved.
- If staff or students discover an unsuitable site it must be reported to the Senior Management Team who will report it to ICT services.

Managing videoconferencing

- Videoconferencing will be managed only using LA systems after discussion regarding appropriateness.

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.
- Staff will not use mobile phones during school time. The sending of inappropriate text messages is forbidden.

- Staff will not use mobile phones in the classroom and any personal mobile phones will be kept in cupboards or lockers. No mobile phone will ever be with a member of staff undertaking intimate care tasks.
- Staff will use the school phone where contact with a student is required.

Protecting personal data

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

Guidelines

Authorising Internet access

- All staff must read and sign the Internet Use Agreement before using any school ICT resources.
- The school will maintain a current record of all staff and student logons who are granted access to school ICT systems. These will be stored in the school safe.
- Management will scrutinize web use through regular weblogs.

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 or the LA can accept liability for the material accessed, or any consequences of Internet access both in school and at home.
- The school should evaluate the implementation of the e-safety policy to ensure that it remains 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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored including use through console games.

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.
- The e safety policy will be available for all staff on the shared area.
- Staff will follow the responsible use of laptops guidelines.
- Staff will have clear procedures for reporting issues.
- Staff will be issued with appropriate good practice guidelines.

Enlisting parents' support

- Parents' attention will be drawn to the school e-safety policy in newsletters, the school prospectus and on the school web site.

Specific Guidance for Responsible use of laptops

Due to the new North Tyneside ICT audit it is important that we understand and comply with their regulations regarding the use of council provided laptops.

Whilst every teacher has been provided with a laptop for use at home and teaching assistants are able to book class laptops for home use consideration must be taken as to the implications of this arrangement, particularly if accessing the internet at home. (Within the remainder of the document laptops for teachers are included within the remit of school laptops.)

Security

Unprotected access to a laptop leaves it open to problems such as possible spyware and/or virus infection. Sensitive information stored may be corrupted and personal information may be leaked through unsecured internet connections.

- *The teacher allocated the laptop or the teaching assistant who has signed out the laptop should be the sole user.*

Other access to the laptop could lead to problems stated before such as virus infection and spyware from popular mail accounts. This could lead to the infection of the North Tyneside system.

- *School data / files should be stored and transported securely.*

In accordance with data protection laws we must ensure that all files / data is secure. Therefore all laptop user accounts should be password protected. Any files / data transported between home / school not on a laptop should be carried on a password protected memory stick or stored in the user's Platform space to be accessed securely over the internet.

- *Care should be taken when using the laptop to connect to the internet at home.*

Any laptop connecting to the internet outside of school needs anti-virus software (provided by school), anti-spyware software and a firewall. The school technician will install these on to all laptops and will monitor virus checking.

Anyone using a wireless connection should always encrypt their signal otherwise the network is open to hacking and therefore unsecured.

- *Staff should not access any webmail accounts (such as Hotmail or Yahoo), instant messaging programmes (such as Messenger) or social network sites (such as Facebook) on a school laptop.*

These provide a back door for viruses and a route for inappropriate material to attach to files. All internet usage should be work related and will be monitored by school.

- *Installation of any software should be authorised by the school technician in accordance with the license agreement.*

By installing their own software, downloads etc staff risk causing errors due to conflicting applications and the risk of contracting viruses and spyware from internet downloads. The technician is there to support staff with any installation.

- *Virus software updates should be carried out at least weekly to ensure up*

to date security. Windows should be set to update automatically.
Support for this is available from the technician whose responsibility it is to monitor updates.

- *Any viruses or spyware infections should be reported to the school Management, or the technician if he is in school, immediately. No connection should be made to the school network until permission has been given to do so.*

Viruses can spread quickly and infect both the school and North Tyneside's network and cause major damage.

- *School laptops must be made available for maintenance.*

Regular maintenance is essential to keep the laptops functioning efficiently and effectively and will be carried out by the school technician at regular intervals throughout the school year.

This policy will operate in conjunction with other policies including those for student behavior and child protection.

The e-safety policy and its implementation will be reviewed bi annually.

Sept 2011