

QEHS e-Safety Policy

With thanks to Kent County Council for permission to use their template.

Last updated 25/03/2009

Contents

1. E-Safety Audit – Secondary / Middle.....	3
2. School e-safety Policy.....	4
2.1 Writing and reviewing the e-safety policy.....	4
2.2 Teaching and Learning	5
2.2.1 Why the Internet and digital communications are important.....	5
2.2.2 Internet use will enhance and extend learning.....	5
2.2.3 Pupils will be taught how to evaluate Internet content	5
2.3 Managing Internet Access.....	6
2.3.1 Information system security.....	6
2.3.2 E-mail.....	6
2.3.3 Published content and the school web site.....	6
2.3.4 Publishing students’ images and work.....	6
2.3.5 Social networking and personal publishing	6
2.3.6 Managing filtering	7
2.3.7 Managing videoconferencing.....	7
2.3.8 Managing emerging technologies	7
2.3.9 Protecting personal data.....	8
2.4 Policy Decisions.....	9
2.4.1 Authorising Internet access.....	9
2.4.2 Assessing risks	9
2.4.3 Handling e-safety complaints	9
2.4.4 Community use of the Internet	9
2.5 Communicating e-Safety	10
2.5.1 Introducing the e-safety policy to pupils	10
2.5.2 Staff and the e-Safety policy.....	10
2.5.3 Enlisting parents’ and carers’ support.....	10

1. E-Safety Audit – Secondary / Middle

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that would contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with NCC guidance?	Y/N
Date of latest update (at least annual):	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have e-safety materials from CEOP and Becta been obtained?	Y/N
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N
Are all students aware of the School's e-Safety Rules?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit has been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	Y/N
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	Y/N

2. School e-safety Policy

2.1 Writing and reviewing the e-safety policy

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

This e Safety policy covers both Queen Elizabeth High School (QEHS) and Hexham Middle School (HMS) through the federation that was formed from September 2008. Some sections are sub-divided where it is necessary to have different content for each school. This has been kept to a minimum.

- The school will appoint an e-Safety coordinator. In some cases this will be the Designated Child Protection Coordinator as the roles may overlap.
- Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by:
- It was approved by the Governors on:
- The next review date is (at least annually):

2.2 Teaching and Learning

2.2.1 Why the 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 high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

2.2.2 Internet use will enhance and extend learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. The schools uses DurhamNet filtering.
 - QEHS also has its own in-house filtering. This in-house filtering is to ensure that content that we deem unacceptable is filtered.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.3 Pupils will be taught how to evaluate Internet content

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

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT system security will be reviewed regularly.
- Virus protection is installed and updated regularly, on both network machines and portable devices.

2.3.2 E-mail

- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, 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 should consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

2.3.4 Publishing students' images and work

- Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs¹.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents/carers.

2.3.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate students in their safe use. Access to the most common ones is prevented.

¹ Need to think about what is in NorTLE, moodle and the biology VLE

- 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, their friends or their location.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

2.3.6 Managing filtering

- The school will work in partnership with NCC, DurhamNet, Becta and the Internet Service Provider to ensure that systems to protect pupils 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. They will take the necessary steps to ensure access is removed.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- At QEHS, an audit of internet access can be carried out. This can be based on a specific URL, on an individual network user, or on a specific workstation.

2.3.7 Managing videoconferencing

- Ideally, videoconferencing should make use of a recognized service, such as that provided by NCC via NorTLE.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the Students' age.

2.3.8 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 management team should note that technologies such as mobile phones or laptops with wireless Internet access (i.e. 3G) 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. The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones is not permitted.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

- The new wireless mesh network at QEHS (due 2009) will enable more access to mobile devices, such as minibooks and students' own devices. The exact extent of this is unknown as QEHS have not been provided with sufficient details by NCC/KBR. The extent of filtering and monitoring needs to be considered carefully when it is installed.

2.3.9 Protecting personal data

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

2.4 Policy Decisions

2.4.1 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.
- Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents/carers will be asked to sign and return a consent form. This form is in all students' planners.

2.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor NCC can accept liability for any material accessed, or any consequences of Internet access.
- The school should 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.

2.4.3 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 Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communicating e-Safety

2.5.1 Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP. This will be delivered through the tutorial programme.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will undergo e-Safety training and a record of attendance will be maintained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to create clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

2.5.3 Enlisting parents' and carers' 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.
- All parents will be given a copy of the Know IT All for Parents DVD as their children arrive at the school. QEHS is working with its feeder schools to ensure this requirement reduces over the near future to only those families moving into the catchment area.
- The school will maintain a list of e-safety resources for parents/carers.