HEXHAM MIDDLE SCHOOL AND QUEEN ELIZABETH HIGH SCHOOL

E-SAFETY POLICY

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils/students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils/students
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Northumberland County Council including the effective management of Policy Central E-Safety Filter and Durham NET

School e-safety policy

- Our e-safety policy relates to other policies including those for ICT, anti-bullying and for child protection.
- QEHS has appointed two named persons to co-ordinate e-Safety at QEHS (Di Harris, Senior Deputy Headteacher and Susan Hope, Business Manager); at HMS the named person is Christine Carruthers.
- The e-Safety Policy and its implementation will be reviewed bi-annually unless there is a significant change in provision.

TEACHING AND LEARNING

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide pupils/students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils/students.

Internet use will enhance learning

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils/students.
- Pupils/students will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use.
- The school will ensure that the use of Internet derived materials by staff and pupils/students complies with copyright law.

Managing Internet Access

- Information system security, School ICT systems capacity and security will be reviewed annually.
- Virus protection will be continuously updated throughout each day.
- Security strategies will be discussed with relevant staff and appropriate bodies.
- E-Safety Filtering is monitored and up to date.
- Web Filtering is monitored and up to date.

E-mail

- Pupils/students may only use approved messaging accounts on the school system.
- Pupils/students must immediately tell a teacher if they receive offensive messages.
- Pupils/students must not reveal personal details of themselves or others in e-communications, or arrange to meet anyone.
- E-communications 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.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number.
- Pupil personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate
- Staff personal contact information will not be published. The contact details given online will be the main switchboard and school contact details of selected key personnel only.

Publishing students/pupils' images and work

- Photographs that include pupils/students will be selected carefully.
- Pupils/students' full names will not be used anywhere on the school website particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils/students are published by the school.
- Pupil/student work can only be published with the permission of the pupil/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.
- Pupils/students will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils/students and parents will be advised of the dangers of the use of social network spaces outside school.
- Pupils/students and parents will be advised the use of social network spaces outside of school will remain the responsibility of the pupils/students and parents.

Social networking – staff guidance

- Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that parents and pupils/students may carry out web and social network service searches to find on-line information about staff, for example; background, interests, career experiences and self-presentation. All staff, perhaps especially new staff in training and induction, are advised to ensure that information available publicly about them is accurate and appropriate.
- Staff must not use internet or web-based communication channels to send personal messages to a child/young person, or their parents. This includes online gaming.
- Staff should not have any secret social contact with children and young people or their parents, for example, using a pseudo name on a social networking site.
- Staff must not give their personal contact details to children or young people, including their parents.
- Staff are to understand that some of their communications may be called into question and may need to be justified.
- Staff are advised not to have online communications with ex-students who have recently left the school and may have friends or family still within the school.
- Staff are strongly advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

Managing filtering

- The school will work with the NCC, DfE and the Internet Service Provider to ensure systems to protect pupils/students are reviewed and improved.
- If staff or pupils/students discover an unsuitable website, it must be reported to the ICT Network Manager who will in turn report information to the e-safety co-ordinators.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Video-conferencing, where available, will be appropriately supervised for the pupils/students' age.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Authorised use of mobile phones will be permitted in lessons. The unauthorised use of cameras of any type is not permitted in school.
- Staff will be issued with a school phone where contact with students is required. Personal mobile phone numbers will not be issued to students or parents.

Protecting personal data

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

ICT access

- All staff will be signposted to the school e-Safety Policy and its importance explained. This is part of the induction process.
- All staff must read and sign the 'Acceptable ICT Use Policy' before using any school ICT resource.
- All pupils/students are asked to sign (and parents to countersign) a copy of the Acceptable ICT Use Agreement. A copy of the completed agreement is kept in each pupil's/student's individual records file. At QEHS, a copy of the agreement is printed in the student planner.
- The school will keep an up to date record of all staff and pupils/students who are granted Internet access.
- Pupils/students' access to the Internet will be bound by the student Acceptable Use Policy
- Everyone will be made aware that Internet traffic can be monitored and can be traced to an individual user.
- E-safety rules will be posted on the intranet and discussed with the pupils/students at the start of each year.
- Pupils/students will be informed that network and Internet use will be monitored in accordance with the student Acceptable Use Policy.
- Parents' attention will be drawn to the school's e-Safety Policy in the school's parents' guide and on the school website. Any suitable e-safety resources that are produced for parents will be made available.
- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with by a senior member of staff.

Protecting personal data

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

The E-safety Policy was agreed by the Education Committee at their meeting on 10 October 2013

Designation	Signature	Date
Chair of Education Committee: Linz Charlton		
Federation Headteacher: Neil Morrison		
Review Date	Autumn 2015	