

MallingHolmesdale

MHF federation

POLICY FOR

E-SAFETY

PERSON RESPONSIBLE

FED DIR OF LEARNING & TEACHING

DATE REVISED

OCTOBER 2010

What is eSafety?

eSafety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism - access to which would be more restricted elsewhere. Children must also learn that publishing personal information could compromise their security and that of others.

eSafety is a safeguarding and child protection issue and The Malling Holmesdale Federation works to ensure that we do our best to protect and educate our students to be safe users of modern digital communication technologies. eSafety depends on staff, governors, parents and – where appropriate - students themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully by all teachers.

Key Responsibilities

MHF's eSafety coordinator is its Director of eLearning.

The eSafety forensic officer is its Network Manager.

eSafety issues are referred to the Child Protection Officer in each school.

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 Malling Holmesdale Federation 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 students. Internet use enhances and extends learning. The school Internet access is designed expressly for student use and includes filtering appropriate to the age of our students.

Digital communications are a vital resource in modern education as they:

- transform teaching and learning and help to improve outcomes for our students, through shared ideas, more exciting lessons and online help for teaching staff;
- engage 'hard to reach' learners and students with special needs support through more motivating ways of learning and more choice about how and where to learn;
- build an open accessible system, with more information and services online for teachers, students, parents and carers as well as the wider community;
- achieve greater efficiency and effectiveness, with online research, access to shared ideas and lesson plans, improved systems and processes in children's services, shared procurement and easier administration.

Risks to Our Students

BECTA identifies four areas in which there are risks for children - content, contact, commerce or culture:

ICT can offer many positive educational and social benefits to young people, but unfortunately there are risks, too. As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal. (Safeguarding Children, BECTA, p.10)

MHF has a clear responsibility to provide a safe eLearning environment through a combination of technical infrastructures and effective policies and practices as well as ensure the safety of our students in virtual worlds whether at school or at home.

Clear boundaries are set for the appropriate use of the internet and digital communications and this is continuously discussed with staff and students. Students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Students are taught how to evaluate Internet content as well as how to be critically

aware of the materials they read and shown how to validate information before accepting its accuracy.

The use of Internet derived materials by staff and by students must comply with copyright law.

Managing Internet Access

MHF ICT system security are reviewed three times a year (at the end of Terms 2, 4 and 6). Virus protection is installed and updated regularly. Internet filtering and software restriction network policies are in place. Where appropriate, security strategies are discussed with the Local Authority.

Email

All students have an email account and can email staff and other students. Students may only use approved e-mail accounts on the school system. Students must immediately tell a teacher if they receive offensive email. In email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming email should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters (email) is not permitted. Misuse of email by students must be reported to vice principals and is managed as part of each school's BfL policy.

Published Content and the Federation's Web Sites

Staff or student personal contact information will not generally be published. The contact details given online should only be the school office or staff school email addresses.

Publishing Students' Images and Work

Photographs that include students will be selected carefully so that individual students 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 photographs. 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.

Social Networking and Personal Publishing

The school will control access to social networking sites, and consider how to educate students in their safe use. 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.

Filtering

The school will work in partnership with Kent LEA, Becta and EIS to ensure that systems to protect students are reviewed and improved. If staff or students discover an unsuitable site, it must be reported to the eSafety 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.

Videoconferencing

Our IP videoconferencing uses an educational broadband network provided by EIS to ensure quality of service and security rather than internet services such as Skype internet video chat. Students should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the students' age.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones should only be used in lessons for lesson-related activities (for example taking photographs or videoing). The sending of abusive or inappropriate text messages is forbidden. The use by students of cameras in mobile phones will be kept under review. Games machines including the Sony PSP, Nintendo Wii and others have Internet access which may not include filtering.

Protecting Personal Data

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

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 students who are granted access to school ICT systems. Students may have internet access only by agreeing to comply with the AUP. Parents/carers will be asked to sign and return the AUP.

Assessing Risks

Our schools 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 KCC can accept liability for any material accessed, or any consequences of Internet access. The school audits ICT use to establish if the eSafety policy is adequate regularly and that the implementation of the eSafety policy is appropriate and effective.

Handling eSafety Complaints

Complaints of Internet misuse will be dealt with by vice principals and the Director of eLearning. 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.

Community Use of the Internet

Where necessary, MHF will liaise with local organisations to establish a common approach to eSafety.

Communicating eSafety

Introducing the eSafety policy to students e-Safety rules will be posted in ICT rooms and published on the VLE. 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.

Staff and the eSafety policy

All staff will be given the School eSafety Policy and its importance explained. Updated copies of Kent LEA's "Safer Practice with Technology" document will be provided to staff at the beginning of each school year and whenever the document is revised. Staff should follow the guidance in the "Safer Practice with Technology" document. 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 leadership and work to clear procedures for reporting issues. Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting Parents' and Carers' Support

Parents' and carers' attention will be drawn to the School eSafety Policy in newsletters, letters and on the school Web site. MHF will maintain a list of esafety resources for parents/carers on the Federation web sites.