e-Safety Policy

Prepared by: R Brice
Created: January 2010

1.0 Introduction

The Unity College e-Safety Policy follows guidance available from DCSF and provides a detailed summary of actions taken by the college to ensure e-Safety. It is revised annually and should be read in conjunction with our Acceptable Use Policy and with material from Lancashire Schools ICT Centre[1], Becta[2] and CEOP[3].

This e-Safety Policy covers the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy summarizes how we will educate all students about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide all users, whether staff or student, in their online experiences.

This e-Safety policy operates in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security plus the Home-School Agreement.

1.1 Scope of policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors and users) who have access to school ICT systems, both in and out of school.

1.2 Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and students;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from the Cumbria and Lancashire Online (CLEO) Network;
- A school network that is compliant with National Education Network standards and specifications.

---

[1] http://www.lancsngfl.ac.uk/esafety/

[2] http://schools.becta.org.uk/index.php?section=is

[3] Child Exploitation and Online Protection Centre http://www.thinkuknow.co.uk

1.3 E-Safety Audit

This audit has been completed by the member of the Senior Leadership Team (SLT) responsible for e-Safety policy. Staff that have contributed to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with CLEO guidance?	**Yes**
Date of latest update (at least annual):	**January 2011**

The school e-Safety policy was agreed by governors on: **2nd February 2011**

The policy is available for staff: **On the intranet and network.**

The policy is available for parents/carers at: **www.unity-college.com**

The responsible member of the Senior Leadership Team is: **Mr S Brice**

The Designated Child Protection Coordinator is: **Mrs A Hodgson**

The e-Safety Coordinator is: **Mrs R Brice**

Has e-Safety training been provided for both students and staff?	**Yes**
Is there a clear procedure for a response to an incident of concern?	**Yes**
Have e-Safety materials from CEOP and Becta been obtained?	**Yes**
Do all staff sign an Accceptable Use Policy on appointment?	**Yes**
Are all students aware of the School's e-Safety Rules?	**Yes through ICT, PSCE, PD time and Yr 7 education but additional awareness will be provided**
Do students know how to report concerns that they might have?	**YES – through this policy and education**
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	**In ICT suites but not other rooms**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	**Yes – gaps to be filled**

Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Yes**
Has an ICT security audit has been initiated by SLT?	**No (need managed service provider input)**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	**Yes - CLEO**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	**Yes**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Yes**
Have appropriate teaching and/or technical members of staff attended training on the CLEO filtering system?	**Yes**
Are staff aware of e-Safety issues and how to deal with them?	**Yes – though further training will be offered**
Do staff know how to conduct themselves professionally online?	**Yes – through this policy, Safeguarding Policy and through the Acceptable Use form they sign**
Are parents/carers given the opportunity to be educated how to keep their children safe online?	**Resources available online via website.**

1.4 Roles and responsiblities

e-Safety Coordinator:

- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff

- monitors the use of the network and email to discover malicious or inappropriate use
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments
- reports regularly to the School Leadership Team

ICT Technician is

The college no longer employs its own ICT Technician as this is outsourced to a managed service. The managed service are responsible for ensuring that :

- the college's ICT infrastructure is secure and is not open to misuse or malicious attack
- the college meets the e-Safety technical requirements outlined in the LCC Security Policy and Acceptable Use Policy
- users may only access the school's networks through a properly enforced password protection policy, in which staff passwords are regularly changed and students passwords can be changed as frequently as needed

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the e-Safety Co-ordinator for
- investigation via their line manager
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and are only carried out using official school systems
- e-Safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-Safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that they follow processes in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school
- are responsible for keeping their network login details and passwords confidential and understand that they are responsible for activity that occurs under their logins

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website / VLE and information about national and local e-Safety campaigns and literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Agreement.
- accessing the school website/VLE in accordance with the relevant school Acceptable Use Policy.

2.0 Writing and reviewing the e-Safety policy

Our e-Safety Policy has been written by the school, building on the Lancashire e-Safety Strategy and government guidance. It has been agreed by senior management and approved by governors.

The e-Safety Policy was created by: … …R Brice … … ……..……

It was approved by the Governors on: … …2nd February 2011…….

The next review date is (at least annually): … January 2012… …….....

2.1 Teaching and learning

2.1.1 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.

2.1.2 Internet use will enhance and extend learning

School Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.1.3 Students will be taught how to evaluate Internet content

We aim to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.2 Managing Internet Access

2.2.1 Information system security

- The College ICT system security will be reviewed regularly.
- Virus protection software is installed and updated regularly.
- Security strategies are discussed with the Local Authority.

2.2.2 E-mail

- Students may only use approved e-mail accounts on the school system.
- 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.

2.2.3 Published content and the school website / VLE

- Staff or student personal contact information will not be published.
- The Head teacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

2.2.4 Publishing students' images and work

- Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.

2.2.5 Social networking and personal publishing

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

2.2.6 Managing filtering

- The school will work in partnership with Lancashire Grid for Learning, Becta and CLEO to ensure that systems to protect pupils are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to thee-Safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.2.7 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 with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones are not permitted to be used during lesson times. 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 Nintendo Wii, 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. Where the college does allow the use of these consoles, they will not be connected to the internet.

- Staff should use a school phone where contact with students is required.

2.2.8 Protecting personal data

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

2.3 Policy Decisions

2.3.1 Authorizing Internet access

- All staff must read and sign the 'Internet & E-Mail Acceptable Use Policy[4]' 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.

- Parents / carers are required to sign a section of the registration details document to authorise their child to access the network and internet

2.3.2 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 LCC can accept liability for any material accessed, or any consequences of Internet access.

- The school will regularly 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.

2.3.3 Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

[4] Attached as Appendix 1

- 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 Communicating e-Safety

2.4.1 Introducing the e-Safety policy to pupils

- e-Safety information 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, based on the materials from CEOP.

2.4.2 Staff and the e-Safety policy

- All staff will be made aware of the School e-Safety Policy and where they can access it.

- Staff will 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 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 and operate within the latest safeguarding guidelines

2.4.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, and on the school website.

- The school will maintain a list of e-Safety resources for parents/carers.