# The Community College Whitstable

# E-Safety Policy

**Agreed by Governors at the Strategy Meeting held on 11th November 2014**

CW

**Mrs C Williams, Chair of Governors** **Date**

HST

**Ms H Sullivan-Tighe, Headteacher** **Date**

Reviewed on 4th November 2014 by Governor, A Pomeroy and Senior Leader Inclusion, L Murphy

The policy will be reviewed every 3 years but will be amended before then if required.

**Next review due:** November 2017

**Contents**

# Rationale

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 students and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The E-Safety Policy is available to all College partners via a home page link and is given to all students and parents/carers to sign upon first induction to the College. We have introduced the Colleges' E-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The College's E-safety policy will operate in conjunction with other College policies such as Behaviour, Curriculum, Data Protection.

- The College has appointed an E–Safety Coordinator.
- The E–Safety Policy and its implementation will be reviewed annually.
- Our E–Safety Policy has been written by the College, building on the KCC e–Safety Policy and government guidance.
- Our College Policy has been agreed by the Leadership Team and approved by Governors and other stakeholders such as the PTA.
- The College has appointed a member of the Governing Body to take lead responsibility for E-Safety

The College E-Safety Coordinator is Deputy Headteacher, Standards & Achievement

# End to End E-Safety

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 in both administration and curriculum, including secure College network design and use.
- Safe and secure broadband from the LA Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

# Teaching and learning

## Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The College has a duty to provide students and staff with quality Internet access as part of their learning and teaching experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The purpose of Internet use in College is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the College's management functions.

## Internet use will enhance learning

- The College Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- 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

- The College will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students use the Internet widely outside College and will need to learn how to evaluate Internet information and to take care of their own safety and security.

# Managing Internet Access

## Information system security

- College ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LA recommended Managed Service Manager
- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

## E-mail

- Students may only use approved e-mail accounts on the College system.
- Students must immediately tell a teacher if they receive 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 organisation should be written carefully and authorised before sending, in the same way as a letter written on College headed paper.
- The forwarding of chain letters is not permitted.

## Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Pupil's work and photographs can only be published with the permission of the pupil and parents/carers.

## Social networking and personal publishing

- The College will block/filter access to social networking sites.
- 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 or their location. Examples would include real name, address, mobile or landline phone numbers, College attended, e-mail address, full names of friends, specific interests and clubs etc.

## Managing filtering

- The College will work with the LA recommended Managed Service, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the E-Safety Coordinator or a member of the College Leadership Team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in College is allowed.
- If necessary, staff will be issued with a College phone where contact with students is required.

## Protecting personal data

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

# Policy Decisions

## Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any College ICT this includes our E-safety Policy.

- The College will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Parents/carers will be asked to sign and return a consent form.

### Assessing risks

- The College 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 College computer. The College cannot accept liability for the material accessed, or any consequences of Internet access.
- The College will audit ICT provision to establish if the E-safety policy is adequate and that its implementation is effective.

### Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the management team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with College child protection procedures.
- Students and parents/carers will be informed of the complaints procedure.

### Community use of the Internet

- The College will liaise with local organisations to establish a common approach to E-safety, if required.

## Communications Policy

### Introducing the E-safety policy to students

- E-safety rules will be posted in all class rooms and the ICT suite and discussed with the students at the start of each term.
- Students will be informed that network and Internet use will be monitored.

### Staff and the E-Safety policy

- All staff will be directed to the College E-Safety Policy on the intranet 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.
- Staff access to social networking sites is prohibited using the College network.
- Staff are directed to refrain from contact with ex-students until at least 1st October in the year after students leave the College, using social networking sites, email or other electronic communication.

### Enlisting parents/carers' support

- Parents/carers' attention will be drawn to the College E-Safety Policy in newsletters and the College brochure.