

## E–Safety Policy

<i>Date of Policy</i>	<i>July 2010</i>
<i>Updated</i>	<i>Jan 2012</i>
<i>Approved by Principal(s)</i>	<i>Yes</i>
<i>Review Date</i>	<i>Jan 2013</i>
<i>Key Staff</i>	<i>Vice Principal, Welfare, Head of Welfare, Heads of House, PTs, Tutors, SLG</i>
<i>Lead on Updating Policy</i>	<i>e-safety coordinator – Head of Welfare - Canterbury</i>

Cats Colleges believe that the use of information and communication technologies in College brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This Policy will assist the College's to implement, monitor and review the College's e-Safety Policy.

This policy has taken into account the guidance on the Kent e-Safety Policies, Information and Guidance website and KCC Children, Families and Education Directorate with Colleges, ASK, Children Safeguard Unit, EIS, SEGfL and Kent Police. It has regard to any advice issued by the Local Safeguarding Children Board.

This policy links into the following policies upheld by the College:

- **Use of ICT, e-safety and Internet Acceptable Use Policy (Students)**
- **Behaviour and Exclusion**
- **Child Protection**
- **Anti-bullying**

## **Contents: Colleges and Settings e–Safety Policy**

### **2.2 Teaching and Learning**

- 2.2.1 Why the use of the Internet is important
- 2.2.2 How Internet use benefits education
- 2.2.3 How the Internet enhances learning
- 2.2.4 How students will learn to evaluate internet content

### **2.3 Managing Information Services**

- 2.3.1 Maintenance of security systems
- 2.3.2 Email management
- 2.3.3 Managing published content
- 2.3.4 Publishing of student images and work
- 2.3.5 Managing social networking and personal publishing
- 2.3.6 Managing filtering systems
- 2.3.7 Managing videoconferencing
- 2.3.8 Managing emerging technologies
- 2.3.9 Protection of personal data

### **2.4 Policy Decisions**

- 2.4.1 Authorisation for internet access
- 2.4.2 Assessing Risk
- 2.4.3 Managing e-safety complaints
- 2.4.4 Internet Use across the community
- 2.4.5 Managing Cyberbullying
- 2.4.6 Managing Learning Platforms and learning environments

### **2.5 Communications Policy**

- 2.5.1 How will the policy be introduced to pupils?
- 2.5.2 How will the policy be discussed with staff?

### **3.0 e–Safety Audit, Contacts and References**

#### **Homestay Internet access Contract**

## **2.1 Who will write and review the policy**

2.1.1 Our e–Safety Policy has been written by the College, building on the KCC e–Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by the Principal

The College will appoint an e–Safety Coordinator who is the Head of Welfare assisted by the Data Manager. The E-safety Coordinator will review annually the e-safety policy and consult staff, students, safeguarding lead and senior management team

## **2.2 Teaching and learning**

### **2.2.1 Why the use of the Internet is important**

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The College has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside College and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in College is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the College’s management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

### **2.2.2 How Internet use benefits education**

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of Colleges, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the DCSF when appropriate;
- Access to learning wherever and whenever convenient.

### **2.2.3 How the Internet enhances learning**

- The College's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The College will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the student's age and maturity.
- 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

### **2.2.4 How students will learn to evaluate Internet content**

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

## **2.3 Managing Information Systems**

### **2.3.1 Maintenance of Security systems**

The College Broadband network includes a cluster of high performance firewalls at each of the Internet connecting nodes. These appliances run industry leading software and are monitored and maintained by a specialist security command centre. The College uses Fortiguard Web Filtering system that is reviewed annually and kept up to date by the Fortiguard ICT Company – monitored by CEG IT Specialists.

The security of the College information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the College's network will be regularly checked.
- CEG Group IT will review system capacity regularly.

### **2.3.2 Email Management**

- Students are encouraged only to use College approved email accounts.

- Students will be encouraged to report to the College if they receive offensive email.
- Students are advised not to give personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in College to external personal email accounts may be blocked if abused.
- Excessive social email use can interfere with learning and will be restricted. Students will not be able to access College emails or internet at night or during times when they should be in lessons or private study
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on College headed paper.
- The forwarding of chain messages is not permitted.
- Staff should only use College email accounts to communicate with students as approved by the Senior Leadership Team. Use of personal email accounts to communicate with students is not permitted.
- Staffs are not permitted to use personal email accounts for professional purposes- (see appendix 3 do's and don'ts email list).

### **2.3.3 Managing Published Content**

- The contact details on the College website will be the College address, email and telephone number.
- Staff or students personal information must not be published.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the College's guidelines for publications including respect for intellectual property rights and copyright.

### **2.3.4 Publishing of student images and work**

- Images that include students will be selected carefully and with their permission
- For students under the age of 18, full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from students will be obtained before any images are electronically published.
- Students work can only be published with their permission.

Please see the Children's Safeguards site, "use of photographic images of children"

[www.kenttrustweb.org.uk/safeguards](http://www.kenttrustweb.org.uk/safeguards) (Policy and Guidance section)

### **2.3.5 Managing of social networking, social media and personal publishing**

Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- The College will control access to social media and social networking sites as appropriate.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, College attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs or wikis will be password protected and run from the College website with approval from the Senior Leadership Team.
- It is not permitted for staff to run social network spaces for student use on a personal basis.
- Students are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

### **2.3.6 Managing filtering systems**

- The College will work with Fortiguard Security Broadband team to ensure that systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL must be reported to the e-Safety Coordinator or CEG Group IT.

The College's broadband access will include filtering appropriate to the age and maturity of students.

- CEG Group will manage the configuration of the filtering system. This task requires both educational and technical experience.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the College believes is illegal will be reported to appropriate agencies such as IWF or CEOP by the e- safety coordinator.

### **2.3.7 Managing videoconferencing**

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information is not permitted on the College Website.
- The equipment must be secure and if necessary locked away when not in use.
- College videoconferencing equipment should not be taken off College premises

without permission.

### **Users**

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the student's age.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

### **Content**

- When recording a videoconference lesson, written permission should be given by all sites and participants where appropriate. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non College site it is important to check that they are delivering material that is appropriate for the lesson.

### **2.3.8 Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by CEG Group IT.
- Staff will be issued with a College phone where contact with students is required. It is not permitted for staff to use their personal mobile phone to contact students.
- Mobile phones should only be used as part of a lesson in College time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- The College has wireless, infrared and Bluetooth communication technologies within the College and the residences.
- Wireless broadband in the residences is managed by the Fortiguard Security filtering system.
- In order to manage the time when the internet access is available to students in residences at the Canterbury Campus the following is currently in place. Residence with students 17 years and under – no internet connection after the hours of 12 midnight. Residence with 18 years and older - no internet connection after the hours of 2 am. During the hours of 10am -3.30 pm there will be no access to the internet at any residences.

### **2.3.9 Protection of 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 Authorisation for Internet access**

- CEG Group IT will maintain a current record of all staff and pupils who are granted access to the College's electronic communications.
- All staff must agree to abide by College IT Policies
- All students will granted Internet access and agree to comply with the e–Safety Rules.

### **2.4.2 Assessing Risk**

- The College will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a College computer. The College cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- CEG group will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

### **2.4.3 Managing e–Safety complaints**

- Complaints of Internet misuse will be dealt with under the College's Complaints Procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded on Magellan which will be sent automatically to CEG Group IT and the e-safety co-ordinator.
- Students and parents will be informed of the College complaints procedure.
- Parents, Agents and students will work in partnership with staff to resolve issues.
- All potentially illegal issues will be discussed with the local Police Safer Colleges Partnership Coordinators and/or Children's Safeguards Unit to establish further action required.
- Any issues (including sanctions) will be dealt with according to the College's disciplinary and child protection procedures.

### **2.4.4 Internet use across the community**

- The College recognises that as a multi-cultural community we will be sensitive to

Internet related issues experienced by students out of the College environment e.g. social networking sites, and offer appropriate welfare support and advice and enable students to contact home via the internet on a regular basis.

#### **2.4.5 Managing Cyberbullying**

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also being used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, College staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

DCSF and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>

- Cyberbullying (along with all forms of bullying) will not be tolerated in College. Full details are set out in the College’s policy on anti-bullying.
- There is welfare support available to any students who have been affected by Cyberbullying.
- All incidents of cyberbullying reported to the College will be recorded.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
- An incident log and racism log is maintained by the College which may be used as evidence. Students are also encourage to keep their own logs when appropriate
- The College will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended at College for the user for a period of time.
  - Parent/carers may be informed.
  - The Police will be contacted if a criminal offence is suspected.
  - The College disciplinary process will be auctioned

#### **2.4.6 Managing learning platforms and learning environments**

An effective learning platform or learning environment offers the College a wide range of benefits to teachers, students and parents as well as support management and administration. It enables collaboration for students and teachers across a global network, can share resources and tools for a range of topics, create and manage digital content and students can develop online and secure e-portfolios. The College intends to move towards the implementation of a full VLE by 2012 in full consultation with relevant bodies. The VLE will be monitored by CEG Group IT and the College. This policy will be reviewed in the light of developments towards the College VLE

When staff or student leave the College their account or rights to specific College areas of existing intranets or Magellan will be disabled or transferred to their new establishment.

### **2.5 Communication Policy**

#### **2.5.1 How the policy will be introduced to students**

E-safety will be introduced at a Student Council meeting, and students have input into e-safety as part of Personal Development as well as being able to have input into the e-safety policy. Key e-safety information is included in the Student Handbook given to all students at the college

Useful e–Safety programmes include:

- Think U Know: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)- **uploading link on intranet**
- Childnet: [www.childnet.com](http://www.childnet.com)
- Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)
- Safe Social Networking: [www.safesocialnetworking.com](http://www.safesocialnetworking.com)
- An e–Safety session will be included in the PSHE, and Personal Development Programme.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

#### **2.5.2 How are staff aware of this policy?**

##### **Discussion:**

Staff have access to College policies online, and copies are placed in the staffroom. Training sessions over the year are an opportunity for staff to engage with safeguarding and e-safety issues and regular short updates to highlight issues are more valuable than longer sessions. Policies are often referred to or highlighted in the College Newsletter to all staff.

All staff must understand that the rules for information systems misuse are specific and instances resulting in disciplinary procedures and dismissal may occur. If a member of staff is concerned about any aspect of their ICT use in College, they should discuss this with their line manager to avoid any possible misunderstanding.

- Appendix 1- e-safety contacts and references***
- Appendix 2 – Homestay computer access contract***
- Appendix 3- Emails do's and Don'ts list***
- Appendix 4- Use of mobile phones in the Classroom***

## ***e-Safety Contacts and References***

Becta: [www.becta.org.uk/safeguarding](http://www.becta.org.uk/safeguarding)

CEOP (Child Exploitation and Online Protection Centre): [www.ceop.police.uk](http://www.ceop.police.uk)

CFE e-Safety Officer, KCC Children Families & Education  
Rebecca Avery email: [esafetyofficer@kent.gov.uk](mailto:esafetyofficer@kent.gov.uk) Tel: 01622 221469

Childline: [www.childline.org.uk](http://www.childline.org.uk)

Childnet: [www.childnet.com](http://www.childnet.com)

Children's Officer for Training & Development, Child Protection  
Mike O'Connell email: [mike.oconnell@kent.gov.uk](mailto:mike.oconnell@kent.gov.uk) Tel: 01622 696677

Children's Safeguards Service: [www.kenttrustweb.org.uk/safeguards](http://www.kenttrustweb.org.uk/safeguards)

Click Clever Click Safe Campaign: <http://clickcleverclicksafe.direct.gov.uk>

Cybermentors: [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

Digizen: [www.digizen.org.uk](http://www.digizen.org.uk)

EIS - ICT Support for Colleges and ICT Security Advice: [www.eiskent.co.uk/ictsecurity](http://www.eiskent.co.uk/ictsecurity)

Internet Watch Foundation: [www.iwf.org.uk](http://www.iwf.org.uk)

Kent e-Safety in Colleges Guidance: [www.kenttrustweb.org.uk/esafety](http://www.kenttrustweb.org.uk/esafety) (Includes a Colleges Audit Tool and Notes on the Legal Framework as part of the PDF versions of this document)

Kent Primary Advisory e-Safety Pages:  
[www.kenttrustweb.org.uk/kentict/kentict\\_home.cfm](http://www.kenttrustweb.org.uk/kentict/kentict_home.cfm)

Kent Public Service Network (KPSN): [www.kpsn.net](http://www.kpsn.net)

Kent Safeguarding Children Board (KSCB): [www.kscb.org.uk](http://www.kscb.org.uk)

Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

Colleges Broadband Team - Help with filtering and network security: [www.eiskent.co.uk](http://www.eiskent.co.uk)  
Tel: 01622 206040

Colleges e-Safety Blog: [www.kenttrustweb.org.uk/esafetyblog](http://www.kenttrustweb.org.uk/esafetyblog)



Teach Today: <http://en.teachtoday.eu>

Think U Know website: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

Virtual Global Taskforce – Report Abuse: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

## Homestay Computer Access Contract

In order for the College to monitor internet provision and ensure compliance with the College’s e-Safety policy students living in Homestay and aged 16 or 17 years will not be allowed to have access to the homestay family’s computer system.

Date: .....

Name of Family: .....

Address of Family: .....

.....

.....

I, ....., agree that student : .....

will not be allowed to access the homestay family’s computer system whilst living with us.

Signed: .....

Date: .....

THIS CONTRACT IS TO BE PLACED ON THE STUDENTS FILE - PLEASE RETURN THIS CONTRACT TO JANICE WILES/GLYNIS BATTER – ACCOMMODATION OFFICER

Do	Don't
<ul style="list-style-type: none"> <li>✓ Keep e-mails short</li> <li>✓ Remember they are never totally confidential</li> </ul>	<ul style="list-style-type: none"> <li>✓ Write anything you are not prepared to account for</li> <li>✓ Send large attachments</li> </ul>
<ul style="list-style-type: none"> <li>✓ Remember that e-mail is a legal document</li> </ul>	<ul style="list-style-type: none"> <li>✓ Send 'blanket' e-mails</li> </ul>
<ul style="list-style-type: none"> <li>✓ Consider carefully who is sent and copied into an e-mail</li> </ul>	<ul style="list-style-type: none"> <li>✓ Have a different subject in the e-mail not covered by the heading</li> </ul>
<ul style="list-style-type: none"> <li>✓ Avoid long discussions – known as 'mail storms'!</li> </ul>	<ul style="list-style-type: none"> <li>✓ Use Bcc to copy e-mails 'blind'</li> </ul>
<ul style="list-style-type: none"> <li>✓ Proofread before you hit 'Send'!</li> </ul>	<ul style="list-style-type: none"> <li>✓ Assume other people will share your sense of humour</li> </ul>
<ul style="list-style-type: none"> <li>✓ Be aware of your audience and the impression they get</li> </ul>	<ul style="list-style-type: none"> <li>✓ Send emotional or sensitive material</li> </ul>
<ul style="list-style-type: none"> <li>✓ Manage your inbox and delete or file old mail</li> </ul>	<ul style="list-style-type: none"> <li>✓ Send it unless it is necessary</li> </ul>

#### Appendix 4-

Mobile phones cannot be used during lessons, supervised study or in the library.

Teachers and supervisors will confiscate the mobile phone of any student who disregards this policy, and give it in to reception where it will be stored in an envelope marked with the student's name, and withheld until 16.00 hours.

If a student repeatedly disregards this rule, the phone may be withheld for a longer period. The student's parents will be informed, and an official warning will be issued in line with our disciplinary procedure.