KINGS COLLEGE
GUILDFORD

E-Safety Policy

2016/17

POLICY REVIEW AND AMENDMENT LOG

Policy Reference: E SAFETY POLICY

Number of pages: 8

Version No.	Reviewed By:	Review Date	Reviewing Governor	Date Approved by Governing Body	Next Review Date
1/2014	Ed Le-Brun	May 2014			May 2016

Kings College Guildford e-safety Policy

Writing and reviewing the e-safety policy

The e-safety policy is part of the school development plan and relates to other policies including those for ICT, anti-bullying and child protection.

- The College will appoint an e-safety co-ordinator. In some cases this will be the Lead Designated Child Protection Officer as the roles overlap. The E-Safety co-ordinator at Kings College is Anna Wallis. Issues surrounding E Safety will also be the responsibility of the Colleges other Designated Child Protection Officers. These are Miss Hamilton; Mr Le Brun; Mr Todd; Miss Jones; Mrs Davis and Miss Dempsey-Miller. Students will be made aware of who they need to speak to should an E-Safety issue arise.
- Our e-safety Policy has been written by the College, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety Policy and its implementation will be reviewed annually.
- The e-safety Policy was revised by Ed Le Brun
- This policy can be found on the College website. Copies can also be obtained from College reception

Teaching and Learning

Why 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 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 students.
- Access to the internet is used to enhance learning. It will do this by allowing access to online revision tools and learning activities. It will also allow students to develop their individual research skills and enhance their work with this research.
- The school internet access is provided by Surrey County Council through a regional broadband contract, which includes filtering appropriate to the age of the 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 safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

- Students will be shown how to publish and present information appropriately to a wider audience.

Students will be taught how to evaluate internet content

- The College will seek to 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 will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon. For students whose parents lack economic or cultural educational resources, the College will build digital skills and resilience acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration will be taken to reduce potential harm.

Managing Internet Access

Information system security

- College ICT systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- **Students and staff 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.
- Staff to student e-mail communication must only take place via a College e-mail address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The College will consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted

Published content on the school web site

- The contact details on the website should be the College address, e-mail and telephone number. Staff or students personal information will not be published.

- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully. In most cases the College will look to use group photographs rather than full face photos of individual children.
- Students' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website.
- Parents should be clearly informed of the College policy on image taking and publishing, both on the College and independent repositories.

Social networking and personal publishing on the College learning platform

- The College will control access to social networking sites, and consider how to educate students in their safe use e.g. use of passwords. This control may not mean blocking every site it may mean monitoring and educating students in their 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 or their location.
- Students must not place personal photos on any social network space provided in the school learning platform.
- Students will learn about 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.
- Students and parents will be advised that the use of social network spaces outside of College brings a range of opportunities; however it does present dangers for secondary aged students.
- Students will be advised to use nicknames and avatars when using social networking sites.
- Students and Staff will receive training, updates and information on developments and issues surrounding Social Media through assemblies, PSHE, Inset days and CPD opportunities.

Managing filtering

- The College will work in partnership with Surrey County Council to ensure systems to protect students are reviewed and improved.
- The College will adopt the use of Smooth Wall to filter internet access in order to protect students from unsuitable materials.

- The College will also adopt the use of Securus Education. This system detects inappropriate content as soon as it appears on screen.
- If staff or students come across unsuitable online materials, the site must be reported to the e-safety Co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents will be used to identify patterns and behaviours of the students. Any material that the school believes is illegal will be reported to appropriate agencies such as the Police or CEOP.

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.
- Mobile phones and associated cameras will not be used during lessons or formal College time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the College.
- College will use a College phone where contact with students is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available in the College.

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 'Staff Code of Conduct for ICT' before using any College ICT resource.
- The College will maintain a current record of all staff and students who are granted access to College ICT systems.
- College students must apply for internet access by agreeing to comply with the College e-safety Rules and Guidelines statement.
- Any person not directly employed by the College will be asked to sign an 'acceptable use of College ICT resources' before being allowed to access the internet from the College site.

Assessing risks

- The College will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a College computer. Neither the College nor SCC can accept liability for the material accessed, or any consequences of internet access.

- The College will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- Students will be expected to use messaging services such as Messenger, BBM and WhatsApp in a sensible and safe manner. Students will not be allowed to use these services during lesson times. Students will be allowed to use these services during morning break and lunch.
- Students who use messaging services at inappropriate times or in a negative way will face sanctions. These include the confiscation of their mobile device(s) or an outright ban on being allowed a mobile device in College. Serious incidents may be deemed to warrant the involvement of the Police.

Handling e-safety complaints

- Complaints of internet misuse must be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedure.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the Colleges' behaviour policy.

Community use of the internet

- All use of the College internet connection by community and other organisations shall be in accordance with the College e-safety policy.
- The College will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

Cyberbullying

Definition of Cyber-bullying

- Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, by individuals or groups of people with the intention to deliberately upset, intimidate or threaten someone else. This can include the following methods:
- Text messages
- Phone calls
- Posts on social media (e.g. Facebook; Twitter; Snapchat)
- E Mail

- Blogs
- Posts on video or photo based websites (e.g. Instagram; Youtube)

Legal Issues

- Cyber-bullying is generally criminal in character and the law applies to cyberspace.
- These laws include the Protection from Harassment Act 1997, which has both criminal and civil provision, the Malicious Communications Act 1988, section 127 of the Communications Act 2003, and the Public Order Act 1986.
- Students and staff will be made aware of the legal implications of cyber-bullying through training. This can take the form of assemblies, PSHE lessons; Inset training or any other methods that the College feels is appropriate.
- E-safety rules surrounding cyber bullying will be posted in all networked rooms.

Guidance for Staff

If staff suspect or are told about a cyber-bullying incident they should follow the protocol outlined below;

Mobile Phones

- Ask the student to show you the evidence of the bullying
- Note clearly everything on the screen relating to the incident and include date, time and any names used.
- If the evidence is a spoken message make a transcript of the message and record the date, time and any names used.
- Tell the student to save the message/image.
- Go with the student to their Head of House or in their absence a member of the Senior Leadership Team.
- If the student informs you that they have received an indecent image **do not open or look at the image.** Inform the student that you need to take their mobile device to the DSL or in their absence the Deputy DSL immediately. Take the student with you to either of these members of staff. In the event of neither being available see the relevant Head of House.
- The Police will be contacted in the case of suspected indecent images.
- If staff suspect that another student possesses material of a bullying nature on their phone under powers included in the Education Act 2011 staff have the specific right to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Computers

- Ask the student to get the material on screen.
- Ask the student to save the material.
- Print off the offending material.
- Take the offending material along with the student to the Head of Year.
- If the student informs you that they have received an indecent image **do not open or look at the image.** Inform the student that they need to log off their account. Take the student to the DSL. In the event of the DSL not being available see the relevant Head of Year.
- The Police will be contacted in the case of suspected indecent images.

Guidance for Students

- If students believe that they or someone else is the victim of cyber-bullying they are to talk to an adult as soon as possible. This could be a parent/carer, tutor, class teacher, Head of Year, Senior Leader or Deputy DCPO.

- Students should not respond to abusive message but save them and report them.
- Students should not delete anything until it has been taken as evidence. This could be in the form of a screen shot or print out. Offensive material will need to be dealt with by the Police.
- As previously stated students should not give out any personal information such as name, phone number or address though e mail, personal publishing, blogs, messaging or when using the Colleges' learning platform.'

Guidance for Parents

- The College will work with parents/carers to ensure that students are aware of the serious consequences of getting involved in cyber-bullying.
- The College will provide parents /carers with relevant information regarding cyber-bullying and how to deal with it.
- Parents/carers should explain to their child the legal issues relating to cyber-bullying.
- If parents/carers believe their child is a victim of cyber-bullying they should save the offending material. Any material of an offensive or threatening nature should see parents/carers contact the Police.
- Parents/carers should contact the relevant Head of House as soon as possible if they suspect their child is being cyber-bullied.
- If an incident occurs outside of College hours the College has the right to take action against any perpetrators.

Sanctions

In the event of cyber-bullying the College will potentially set one of the following sanctions;

- Removal of the right to have a mobile device in College
- Suspension of College ICT account
- Internal Exclusion
- Temporary External Exclusion
- Police involvement

Communications Policy

Introducing the e-safety policy to students

- Appropriate elements of the e-safety policy will be shared with students.
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for students. This should be addressed each year as students become more mature and the nature of newer risks can be identified.
- E Safety issues will be covered in PSHE, ICT and Computing. Registration periods and assemblies will also be used to highlight issues termly. Outside agencies will also be used to develop student’s awareness throughout the year and the College will be involved in initiatives such as Safer Internet Day in February.
- Topics covered will include issues such as sexting and cyber-bullying.
- Year 7 will receive initial e-safety training during the first two weeks of term.

Staff and the e-safety policy

- All staff will be given the College e-safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the e-safety Policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that monitor filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will receive regular training and updates regarding e-safety. It will be part of staff CPD every year as part of the induction process.
- Staff will also be required to be involved in activities such as Safer Internet Day to help raise awareness of the importance of e-safety.

Enlisting parents support

- Parents' and carers' attention will be drawn to the College e-safety Policy in newsletters, the College brochure and on the College website.
- The College will ask all new parents to sign the student/parent agreement when they register their child with the College.
- Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.
- Parents should be given e-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.
- In order to achieve this there will be a regular Safeguarding feature in the College newsletter that will focus on issues surrounding e-safety. Sessions will also be held at Parents Evening’s to help develop parents understanding of the issues surrounding e-safety. Attendance at these sessions will be recorded and monitored.

This Policy will be reviewed every two years