

# HAMPTON COLLEGE: E-SAFETY POLICY

---

## Purpose

The Hampton College E-Safety Policy will:

- allow young people to develop their own protection strategies for when adult supervision and technological protection are not available
- give information on where to seek help and how to report incidents
- help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online
- provide guidelines for Staff, parents / carers and other relevant stakeholders on safe practice
- ensure we regularly monitor and review our policies with those stakeholders
- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

It is the responsibility of everyone using the school's ICT systems to read, understand and implement this policy.

The E-Safety Policy will be reviewed annually.

## Teaching and Learning

### **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 part of the statutory curriculum and a necessary learning tool for staff and students.

### **Internet use will enhance and extend learning**

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

# HAMPTON COLLEGE: E-SAFETY POLICY

---

## **Students will be taught how to evaluate Internet content**

- Schools should ensure that the use of Internet derived materials by staff and by 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.

## **Managing Internet Access**

### **Information system security**

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

### **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.

### **Published content and the school web site**

- Staff or student personal contact information will not generally be published. The contact details given online will be the school office.

### **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.

# HAMPTON COLLEGE: E-SAFETY POLICY

---

- 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.

## Managing filtering

- The school will work in partnership with PCC, Becta and the Internet Service Provider 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 e-Safety 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.

## 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 Leadership Team are aware 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 allowed in school.
- Staff will be issued with a school 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 'Staff Acceptable Use Agreement' 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 are granted Internet access individually by agreeing to comply with the Student Acceptable Use statement which parents/carers will be asked to sign and return to the school.

### 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 PCC can accept liability for any material accessed, or any consequences of Internet access.
- The school will 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.

# HAMPTON COLLEGE: E-SAFETY POLICY

---

## Handling e-safety complaints

- Complaints of Internet misuse within the school will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure via the school website.

## Communicating e-Safety

### Introducing the e-safety policy to students

- e-Safety rules 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 for staff and students.

### Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- 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 within 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 will take care always to maintain a professional relationship.

### Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.

APPROVED BY GOVERNORS:

---

SIGNATURE	NAME	DATE
-----------	------	------