



**CARISBROOKE HIGH SCHOOL  
E-SAFETY PROCEDURES**

## **1. Introduction**

- 1.1 The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- 1.2 The school will appoint an e-Safety coordinator and this may be the Designated Child Protection Coordinator as the roles may overlap.
- 1.3 This e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.

## **2. Teaching and learning**

### **2.1 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 students.

### **2.2 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.

### **2.3 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.

## **3. Managing Internet Access**

### **3.1 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.

### **3.2 E-mail**

- Students may only use allocated email provision or approved e-mail providers on the school system (contact the helpdesk for up-to-date information).
- Students must immediately tell a teacher if they receive offensive e-mail.

## CARISBROOKE HIGH SCHOOL E-SAFETY PROCEDURES

- 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.

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

- Staff or student personal contact information will not be published. The contact details given online will be for school business reasons only.
- The head teacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

### 3.4 **Publishing students' images and work**

- Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused.
- With the exception of specifically parentally authorised news articles, 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.

### 3.5 **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 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.

### 3.6 **Managing filtering**

- The school will work in partnership with Isle of Wight Council, 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 responsible teacher or the ICT helpdesk.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### 3.7 **Managing videoconferencing**

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than directly using the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' age.

### 3.8 **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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras and camera mobile phones will be kept under review. Students must not take photos or videos of other students or members of staff without permission.
- Games machines including the 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.
- Staff will be issued with a school phone where contact with students is required; staff must not store students' numbers on mobile phones.

### 3.9 **Protecting personal data**

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

## **4. Policy Decisions**

### 4.1 **Authorising Network and Internet access**

- All staff and volunteers must read and sign the 'Acceptable Computer Use and Internet Access Policy for Staff' [Appendix A] before using any school ICT resource.
- All students must read and sign the 'Acceptable Computer Use and Internet Access Policy for students' [Appendix B] 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.
- On request parents/carers may opt-out of internet access for their child.

### 4.2 **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 Isle of Wight Council 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.

#### 4.3 **Handling e-safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- 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 school attached Police Community Support Officers (PCSOs) to establish procedures for handling potentially illegal issues.

#### 4.4 **Community use of the Internet**

- The school will liaise with local organisations to establish a common approach to e-safety.

### **5. Cyberbullying**

5.1 Cyberbullying takes different forms: threats and intimidation, harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images), and manipulation.

5.2 Cyberbullying, like all bullying, is taken very seriously. It is never acceptable, and a range of Education Acts and government guidance outline schools' duties and powers in relation to bullying. The Education and Inspections Act 2006 (EIA 2006) includes legal powers that relate more directly to cyberbullying. It outlines the power of head teachers to regulate the conduct of students when they are off-site, and provides a defence in relation to the confiscation of mobile phones and other items.

5.3 Although cyberbullying is not a specific criminal offence, there are criminal laws that can apply in terms of harassment, and threatening and menacing communications, therefore cyberbullying will be dealt with as any other offence and the school will contact the police if they feel that the law has been broken.

5.4 It is not acceptable to write comments, make or upload images or videos of any individual without their express written permission. This includes members of staff, visitors, the general public and any other student(s) of this or any other school.

5.5 The school will record and monitor incidents of cyberbullying in the same way as all other forms of bullying and the same sanctions will apply. Please see the school disciplinary policy for further information.

5.6 The school has adopted government guidance and a best practice approach to cyberbullying further details on this guidance can be obtained from:

<http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying>

### **6. Communicating e-Safety**

**6.1 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.
- Awareness of e-safety will be raised through the production and distribution of Childnet International Guides for parents, carers, students and teachers.
- A programme of training in e-Safety will be developed, possibly based on the materials from Child Exploitation and Online Protection Centre (CEOP).

**6.2 Staff and the e-Safety policy**

All staff will be given the School e-Safety Policy and its importance explained.

- Staff must 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 students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff should not publish personal information or photos of themselves or family members on social networking sites. Comments and media content posted on social networking sites is publicly available and could be misused or misinterpreted and may damage the individuals professional image and compromise their position within the school.

**6.3 Enlisting parents' and carers' support**

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