

# Congleton High School E-Safety Policy



## 2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Safeguarding Policy.

The e-Safety Co-ordinator is Mrs G Taylor (Child Protection Lead Officer)

- Our e-Safety Policy has been written by the school, building on the Cheshire e-Safety Policy and government guidance. It has been agreed by senior leadership and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

## 2.2 Teaching and learning

### 2.2.1 Why Internet use is 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.

### 2.2.3 Internet use will enhance learning

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

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

- The school 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.

## 2.3 Managing Internet Access

### 2.3.1 Information system security

- School ICT systems and security will be reviewed regularly.
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
- We have adopted Cheshire East security standards.

### 2.3.2 E-mail

- 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.

- Students should only use school e-mail to communicate with staff
- The forwarding of chain letters is not permitted.

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

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

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

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site or Blog, 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.
- Students' work can only be published with the permission of the student and parents.

### **2.3.5 Social networking and personal publishing**

- School will block access to Facebook and educate students in the safe use of social networking sites that could aid their education.
- Students will be advised never to give out personal details of any kind which may identify them or their location.

### **2.3.6 Managing filtering**

- The school will work with the LA, 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 Network Manager who should be known to all members of the school community.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **2.3.7 Managing videoconferencing**

- Videoconferencing will be appropriately supervised for the students' age.

### **2.3.8 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.
- Mobile phones will not be used during lessons or formal school time, unless permission is given by the staff concerned, in line with the CHS Mobile Phone Policy
- The sending of abusive or inappropriate text messages is forbidden
- Staff will not use personal equipment or non school personal electronic accounts when contacting students. This includes becoming 'friends ' with any student on a social networking site.

### **2.3.9 Protecting 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 Authorising Internet access**

- All staff, through signing the school's Safeguarding procedures, will use correctly the IT systems in school.
- All students and their parents must read and agree to the 'Students' Safety Rules' (in Student Planners).
- Parents will be asked to agree to and sign the Student Planner with respect to the 'Students' Safety Rules'.

### **2.4.2 Assessing risks**

- The school 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 school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit regularly ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

### **2.4.3 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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

### **2.4.4 Community use of the Internet**

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

## **2.5 Communications Policy**

### **2.5.1 Introducing the e-safety policy to students**

- E-safety rules will be posted in all networked rooms and discussed with the students at the start of each year.
- Students will be informed that network and Internet use will be monitored.
- The lead teacher in ICT is CEOP trained and students complete units of work in KS3 that promote and raise awareness of e-safety.

### **2.5.2 Staff and the e-Safety policy**

- All staff will be given the School e-Safety Policy 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.

### **2.5.3 Enlisting parents' support**

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school Prospectus and on the school Web site.