HEOLDDU COMPREHENSIVE SCHOOL

E-Safety Policy

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The e-Safety coordinator is Mrs L Prosser who is also the Designated Child Protection Coordinator, as the roles may overlap.

Our e-Safety Policy has been written by the school, building on BECTA and WAG guidance. It has been agreed by senior management and is to be approved by governors.

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 a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning
The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content
Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils 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
The school does not at present provide e-mail accounts for its students. This may be provided in the near future through an arrangement with Caerphilly CBC.

Staff email is provided by Caerphilly CBC and they must comply with the contents of the AUP.

Published content and the school web site
Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images and work
On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Social networking and personal publishing
The school will control access to social networking sites, and consider how to educate students in their safe use.
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.

Managing filtering

The school will work in partnership with Caerphilly CBC to ensure that systems to protect pupils are reviewed and improved. Caerphilly CBC will provide filtered Internet content and this will be enhanced with the use of Impero Software purchased by the school.

If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or ICT Coordinator.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and school suitability. 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. The use of mobile phones by students is to be discouraged, and at the present time the normal policy is to confiscate the phone.

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 Acceptable Usage Policy before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Students must comply with the Responsible Internet Use statement when they log on to the network and by signing in the pupil planner.

Parents/carers will be asked to sign a consent form in the pupil planner.

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 Caerphilly CBC can accept liability for any material accessed, or any consequences of Internet access.

The school should 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.

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 child protection procedures. Students and parents will be informed of the complaints procedure.

Communicating e-Safety

Introducing the e-safety policy to pupils
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.
In their first term in Heolddu, year 7 pupils will study a unit of work on e-Safety, based on the materials from CEOP.

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 should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must 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 brochure and on the school Web site.
The school will maintain a list of e-safety resources for parents/carers.

Signed: ………………………… (Headteacher)   Signed: ………………………….. (Chair of Governors)

Date: …………………………   Date: …………………………..

Review date: ………………………..