Polisi E-ddiogelwch/ E-Safety Policy

Ysgol Bancyfelin, Ysgol Llangain ac Ysgol Llansteffan

E-safety policy

This policy protects pupils and educates them in responsible ICT use.

1.1 Introduction

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.

The school has an e-Safety Coordinator- Mrs Trefina Jones

Our e-Safety Policy has been written by the school and reflects the Carmarthenshire e-Safety Guidance. It has been agreed and approved by members of staff and the governors.

The e-Safety Policy and its implementation will be reviewed annually.

1.2 Teaching and learning

1.2.1 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 pupils.

1.2.2 Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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

1.2.3 Pupils will be taught how to evaluate Internet content

The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

School ICT systems capacity and security are reviewed regularly.

Virus protection is updated regularly.

Security strategies are discussed with Carmarthenshire County Council.

1.3.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive an offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

1.3.3 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 pupils' personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupils' images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' 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 pupils are published on the school Web site.

Pupils' work can only be published with the permission of the pupil and parents.

1.3.5 Social networking and personal publishing

The school will block / filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind that may identify them or their location.

1.3.6 Managing filtering

The school works with the Carmarthenshire County Council IT Services to ensure systems to protect pupils are robust and regularly reviewed.

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

1.3.7 Managing videoconferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

1.3.8 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. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

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

1.4 Policy Decisions

2.4.1 Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

The school maintains a current record of all staff and pupils who are granted Internet access.

Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

1.4.2 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 CCC can accept liability for the material accessed, or any consequences of Internet access.

The school audits ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

1.4.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the Headteacher

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.

Discussions will be held with the Education & Children's Service and / or Police to establish procedures for handling potentially illegal issues.

1.4.4 Community use of the Internet

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

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

E-safety rules will be clearly posted where there is computer access and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

1.5.2 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 brochure / prospectus and on the school Web site.