YSGOL GYNRADD GYMUNEDOL

SWISS VALLEY

COMMUNITY PRIMARY SCHOOL

YSGOL SWISS VALLEY SCHOOL

Mae rhaid mentro cyn cael dim

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) E-SAFETY

Our ICT Vision
Our aim is to safely teach todays' children
tomorrows' technologies in
and beyond the classroom.

School E-Safety Policy

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile devices as well as collaboration tools and personal publishing. It highlights the need to educate learners about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The Core e-Safety Policy

This Swiss Valley C.P. School e-Safety Policy has been adapted from the Carmarthenshire Schools e-Safety Core Policy, which provides the essential minimum for a school e-safety policy.

The Carmarthenshire Schools e-Safety Core Policy and Guidance notes available on Amdro provided the guidance to fully discuss e-safety issues by the staff, the ICT Development Team, the SMT and School Governors.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Carmarthenshire County Council including the effective management of Censornet filtering.
- National Education Network standards and specifications.

Further Information

School Improvement Service

Primary IT Consultant

IT Helpdesk

e-Safety materials and links as published on Amdro

Becta Curriculum e-safety advice

School e-safety policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Safeguarding, bullying and for child protection.

- The school has an e-Safety Coordinator. This is the Headteacher who is also the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school ICT Leader and reflects the Carmarthenshire e-Safety Guidance. It has been agreed by the staff, senior management and approved by governors.

Teaching and learning

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 learners.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of learners.
- Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Learners will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and learners complies with copyright law.
- Learners 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 systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly (via county IT services).
- Security strategies will be discussed with Carmarthenshire County Council.

E-mail

- Learners may only use approved e-mail accounts on the school system.
- Learners must immediately tell a teacher if they receive offensive e-mail.
- Learners 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.

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 learners' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil’s images and work

- Photographs that include learners will be selected carefully and will not enable individual learners to be clearly identified.
- Learners’ 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 learners are published on the school Web site.

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.
- Learners will be advised never to give out personal details of any kind that may identify them or their location.
- Learners and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged learners. However, when situations arise due to use of social networking sites at home, appropriate guidance will be given to learners on how to conduct themselves safely online.

Managing filtering

- The school will work with the Carmarthenshire County Council ICT Services to ensure systems to protect learners are robust and regularly reviewed.
- If staff or learners discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- The ICT Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- IP videoconferencing and webinars should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Learners should ask permission from the supervising teacher before making or answering a videoconference or webinar call.
- Videoconferencing and webinars will be appropriately supervised for the learners’ age.

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.
- Staff will be issued with a school phone where contact with learners or staff is required i.e. school visits

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 ICT Use Agreement’ before using any school ICT resource.
- The school will maintain a current record of all staff and learners who are granted Internet access.
- In The Foundation Phase, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

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 will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is 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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Learners and parents will be informed of the complaints procedure.
- Discussions will be held with the Education & Children’s Service and / or Police to establish procedures for handling potentially illegal issues.

Community use of the Internet

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

Communications Policy

Introducing the e-safety policy to learners

- E-safety rules will be clearly posted where there is computer access and discussed with the learners at the start of each year.
- Learners will be informed that network and Internet use will be monitored.

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.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure / prospectus, in open evenings and on the school Web site.

Revised and updated November 2014