YSGOL PENMORFA

ICH DIEN

Making the most of everyone.

# *E-Safety Policy*

**Policy Adopted June 2014**

**Policy Reviewed on 16th January 2023**

**Policy Valid until March 2025**

**Signed: (Chair of Governors)**

# Ysgol Penmorfa

# Policy for e-safety

E-safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies including:

- DCC Safeguarding Policy
- Pupil Behaviour
- Bullying Prevention
- Child Protection
- PSE Policy
- Curriculum
- Data Protection and Security

**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 and clear guidance.

• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

• To teach the children to use the internet safely under supervision, developing their skills and understanding in order for them to manage their own risk as they use the internet independently.

• Safe and secure broadband including the effective management of filtering.

• A member of staff being responsible for the implementation and monitoring of this e-safety policy.

• All staff to be involved in the implementation and management of e-safety, being vigilant to both their use of technology and the monitoring of pupils use in the context to their safeguarding responsibilities.

The purpose of this policy is to:

• Through consultation with pupils establish the ground rules we have at Ysgol Penmorfa for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

• Describe how these fit into the wider context of our discipline and PSE policies.

• Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

• Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

**Teaching and learning**

• 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.

• The school Internet access is designed expressly for teacher reference and 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

• 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 (Screen time for children is limited and carefully scheduled in light of medical advice)

• HWB is a learning platform for educators and learners to share resources, knowledge and experience across the whole of Wales. All pupils and parents are expected to sign up to the HWB/internet user agreement.

- The children are taught the benefits of mobile technologies and how to use them safely.
- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid the establishment and the future development of the school's e-safety rules.
- However, staff are aware that some pupils may require additional support or teaching including the adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

**Managing Internet Access**

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.

**E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e- mail.
- Pupils must not send offensive of inappropriate e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.
- The school reserves the right to access pupil e-mail accounts if a concern is raised regarding inappropriate content.
- Pupils must not attempt to gain access to another person/pupil account.
- Pupils are taught not to share passwords with other people.

**School web site**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupil's personal information are not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- To ensure the safeguarding of all pupils, photographs are only published with the pupil's first names.

**Cyber Bullying** (a form of bullying through the use of ICT)
An effective whole school approach to the prevention of cyber bullying should include:

- An agreed whole school understanding of cyber bullying
- Talking about cyber bullying
- Encouraging children to report any incidents of cyber bullying
- Promoting the positive use of technology
- Regularly monitoring the impact of this policy and the teaching and learning of ICT.

Responding to the incident of cyber bullying should be dealt with using the existing behaviour and bullying prevention policies and procedures.
If cyber bullying takes place outside of school and has a negative impact on the orderly running of the school and/or might pose a threat to another pupil during school time or to a member of staff then the head teacher may take reasonable steps to mediate between the parties.

**Managing filtering**

- If staff or pupils discover an unsuitable site, it must be reported immediately to a member of staff and/or the head teacher.
- The head teacher ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.

**Managing video conferencing** (Skype/facetime)

- Video conferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing is appropriately supervised for the pupils' age.

**Managing emerging technologies**

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.

**Protecting personal data**

- Personal data is recorded, processed, transferred and made available according to GDPR as set out by DCC.

**Assessing risks**

- The school takes all reasonable precautions to ensure that users' access only appropriate material by using Denbighshire's filtering system.
- The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

**Handling e-safety complaints**

- Serious complaints of e-safety misuse are recorded by the member of staff who receives the complaint and then reported to the head teacher.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the school's child protection procedures, DCC Safeguarding Policy and All Wales Child Protection Procedures.
- The school's Complaints Policy is available to all parents.

**Communications**

Introducing the e-safety policy to pupils

- E-safety rules are discussed with the pupils at the start of each year.
- As part of the school's e-safety work all pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

**Staff and the e-safety policy**

- All staff have copies of the school's e-safety Policy and know its importance.
- Staff are aware of their responsibility to safeguard all pupils in their use of technology in learning.

**Enlisting parents' support**

- Parents' attention is drawn to the school's e-safety Policy in newsletters, and on the school Web site.
- Parents are requested to follow the school's complaints procedure and not use social media.

**Working with the Police**

- The school works in partnership with the Schools Community Police Officer as part of the schools e-safety work.

- Some forms of cyber bullying behaviour may involve criminal offences and in these cases the school will contact the SCPO in line with the school's bullying prevention policy.

This policy will be reviewed bi-annually by the governors and staff or in light of new guidance.