Ysgol Penmorfa

E-Safety Policy

Introduction

The internet has become a vital source of information across the curriculum and is an excellent tool for learning. However, as the technology develops, the hazards to the well being of children and staff must be safeguarded.

E- safety

Our e-safety strategy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. e-safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. However, much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people.

In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others. Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to groom children.

We try to make it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is unauthorised.

Classifying the risks

The Byron Review classifies e-safety risks as involving content, contact and conduct, illustrating that the risk element involved in using new technologies is often determined by behaviours rather than the technologies themselves. A child may be a recipient, participant or actor in online activities posing risk, as illustrated below:

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Adverts Spam Sponsorship Personal Info	Violent/Hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact Child as participant	Tracking Harvesting Personal Info	Being bullied, harassed or stalked	Meeting strangers or being groomed	Self harm Unwelcome persuasions
Conduct Child as actor	Illegal downloading, Hacking, Gambling, Financial scams, Terrorism	Bullying or harassing another	Creating or uploading inappropriate material	Providing misleading info/advice

Aims

The aim of this policy is to define practices that ensure that children and staff:

- are protected from information or images which may be offensive/ damaging to their emotional well being
- are not exploited by persons external to the school
- are not exposed to bullying or harassment on line
- receive accurate and up to date information about how to use the internet safely both inside and outside school.

Provision

All classroom PCs and those in the computer suite are linked through a server to the internet. The administration PCs and the curriculum machines are maintained by Gaia.

Firewall

An internet security system is in place in which inappropriate websites and blocked in order to prevent children from being exposed to information and images that could be damaging to their emotional well being.

Responsibilities of staff

- Staff are obliged to sign a declaration to ensure that they will not refer to the children, staff or the school whilst on line through social networking sites or other media. The declaration includes clear guidelines which staff must follow.
- Staff are advised not to refer to the children, staff or the school whilst on line through social networking sites or other media.
- Staff must also be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source. Any allegation of inappropriate behaviour must be reported to senior management and investigated with great care. An innocent explanation may well exist. E-mail and text messaging all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur, or communications can be misinterpreted.

Safe use of the internet

Most Internet use in schools is safe, purposeful and beneficial to learners. There is always an element of risk. Even a seemingly innocent search can occasionally turn up links to adult content or violent imagery.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content.

If this occurs: **Close or minimise the image or window immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Report the matter to the Headteacher.**

In view of the risks, pupils should be supervised at all times when using the Internet. All staff should be aware that networked computers are generally online at all times when a user is logged on.

Search engines

For most curriculum-related research, there is no need to use an unfenced search engine. The danger is that these will accept inappropriate keywords. There may be no need for pupils to download images, as long as an adult downloads the images before the lessons and stores them in a shared folder.

Please note that NO filter-based search engine is completely safe.

Child Training

The children are given instruction in internet safety by class teachers and by our community police officer PC Catrin Brown. This covers issues such as:

- The need for regulating the time spent using a PC
- The legal and emotional implications of bullying on line
- The dangers of using social networking sites

The BBC Primary Internet Chat Guide contains a range of carefully designed teaching packs for KS2 and KS3. There are games and advice for children and young people and a downloadable ChatGuide booklet for parents.

CEOP's 'think you know' programme is an excellent resource and contains age related e-safety advice with interactive games and activities for all children and young people from the age of 5 upwards.

School responsibility

- The person with e-safety responsibility is the Headteacher (child protection officer). The Headteacher will maintain the e-safety policy, manage e-safety training and keep abreast of local and national e-safety awareness campaigns.
- The Headteacher will review the e-safety strategy annually and revise it to ensure that it is current and considers any emerging technologies.
- To ensure that pupils and staff are adhering to the strategy and related policies, any incidents of possible misuse will be investigated.
- We will include e-safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupil need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable Use Policy.
- Pupils and Parents should be asked to sign and return the Acceptable Use Policies. (Appendix A and B)

Appendix A

YSGOL PENMORFA

Our E-Safety Rules

- The school owns the PC's and will set rules for how you use them.
- You will only be able to use the PC's or the Internet when a teacher or other member of staff is present.
- You will be able to use the Internet, but only sites chosen by the school.
- You will only be allowed to play games chosen by the school.
- You will only be able to use safe search engines.
- The PC and Internet use may be monitored by the school and your parents or carers told if you are not using them safely.
- If you see any pictures or file while using the school computers that make you feel uncomfortable report it to a teacher or member of school staff.
- Do not give anybody your name, address or name of your school to anybody you speak to on the Internet.
- Do not arrange to meet someone you meet on the Internet.
- Do not send messages that you know will upset someone.

Pupil Agreement[1]:

I have read the rules above and agree to follow them.

If I do not use the computers or the Internet safely the school will tell my parents or carers and I may not be allowed to use the PC's or the Internet in future if it does not improve.

Signed:…….Date: ……..

[1] To be completed by KS2 pupils only. For Foundation Phase pupils, parental consent only is sufficient.

Ysgol Penmorfa

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

- I understand that it may be an offence to use any of the school ICT systems for any other purpose than permitted by its owner.
- I appreciate that ICT resources includes a wide range of systems or devices, including PC's, laptops, notebooks, mobile phones, palmtop computers, digital cameras, e-mail or specific IT systems. This could also include the use of personal devices if used for school or educational purposes.
- I understand that my use of school ICT resources, Internet and e-mail may be logged and monitored to ensure compliance with relevant policies.
- I accept that I am responsible for the use of my user ID and password and will keep my password secure, not write it down and not disclose it to any other person.
- I will not install software or hardware without explicit permission from the ICT Department or the Headteacher and will respect copyright and intellectual property rights.
- I will ensure that personal data is stored securely and is used appropriately.
- I will ensure that I will make no reference to school, pupils or colleagues whilst on line or on social media sites such as Facebook.
- I will report any incidents of concern regarding children's safety to the Headteacher.
- I will promote e-safety at all times with pupils under my supervision or care and will help them to develop a responsible attitude to ICT use, communications and publishing.
- The School may exercise its right to monitor the use of the its information systems and Internet, to intercept e-mails and to delete any inappropriate material it finds where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I accept that non-compliance with the relevant school policies as directed by the Headteacher may lead to disciplinary action, including dismissal.

I have read, understood and accept the Code of Conduct for ICT.

Signed: …….

Print name: ……..…….

Date: ……..

Ysgol Penmorfa

Volunteers and Students on placement Code of Conduct for ICT

To ensure that volunteers and students on placement are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

- I understand that it may be an offence to use any of the school ICT systems for any other purpose than permitted by its owner.
- I appreciate that ICT resources includes a wide range of systems or devices, including PC's, laptops, notebooks, mobile phones, palmtop computers, digital cameras, e-mail or specific IT systems. This could also include the use of personal devices if used for school or educational purposes.
- I understand that my use of school ICT resources, Internet and e-mail may be logged and monitored to ensure compliance with relevant policies.
- I accept that I am responsible for the use of my user ID and password and will keep my password secure, not write it down and not disclose it to any other person.
- I will not install software or hardware without explicit permission from the ICT Department or the Headteacher and will respect copyright and intellectual property rights.
- I will ensure that personal data is stored securely and is used appropriately.
- I will ensure that I will make no reference to school, pupils or colleagues whilst on line or on social media sites such as Facebook.
- I will report any incidents of concern regarding children's safety to the Headteacher.
- I will promote e-safety at all times with pupils under my supervision or care and will help them to develop a responsible attitude to ICT use, communications and publishing.
- The School may exercise its right to monitor the use of the its information systems and Internet, to intercept e-mails and to delete any inappropriate material it finds where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I accept that non-compliance with the relevant school policies as directed by the Headteacher may lead to disciplinary action, including dismissal.

I have read, understood and accept the Code of Conduct for ICT.

Signed: …….

Print name: ……..…….

Date: ……..