

Ysgol Penyffordd



e-Safety POLICY

To inspire a love of learning, now and forever.

e-Safety Policy

Ysgol Penyffordd



Introduction

Through these elements Digital technology in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Ysgol Penyffordd has identified the need to embrace the use of digital technology in order to equip our pupils with the digital competencies to access lifelong learning and enhance their employment opportunities in the future. At Ysgol Penyffordd learners will engage with what it means to be a conscientious digital citizen who contributes positively to the digital world around them and who critically evaluates their place within this digital world. They will be prepared for, and ready to encounter, the positive and negative aspects of being a digital citizen. They will be given opportunities to develop strategies, and tools, to aid them as they become independent consumers and producers.

Roles and Responsibilities:

eSafety is an important aspect of strategic leadership within the school, the Digital Lead, Headteacher and SMT have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Digital Lead is responsible for coordinating eSafety at Ysgol Penyffordd and keeping all staff updated. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice. Ysgol Penyffordd has appointed a member of the Governing Body to take lead responsibility for eSafety via the role of eSafety Governor.

eSafety and staff

- Our staff receive regular updated information and training on eSafety issues when required from the Digital Lead or outside agencies
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know the reporting procedure for any concerns
- All staff have agreed to and signed the school's Acceptable Use Agreement/code of conduct
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

eSafety and learners:

- All learners must sign pupil Acceptable Use Agreement
- Delivery of digital citizenship is a cross-curricular responsibility as part of the Digital Competence Framework. In addition, specific citizenship lessons (Digital Literacy resource from Hwb) will be taught by all staff each half term)
- The eCadet (KS2) and mini eCadet (FP) programme are established across the school to raise the awareness of digital citizenship via peer collaboration and pupil voice via assemblies, delivering lessons and drop in sessions. They also feedback to governors during meetings to keep them informed of school developments.

eSafety and parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement along with their child
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used online e.g. on the school website, blogs, YouTube, and Twitter. Parents are to inform the Headteacher in writing if they do NOT give consent.
- The school website contains useful information and links posted by the Digital Lead and the eCadets to support online learning and eSafety to inform and update parents.

Community use of the internet

External organisations are not allowed access to the school's digital facilities without permission from the Headteacher.

Cyberbullying management

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details and procedures are set out in the school's policy on anti- bullying and behaviour policy. This is also supported by our Community Social Media Code of Conduct.

Managing Internet Access

Email

Email is an essential means of communication for both staff and pupils. Ysgol Penyffordd believe that pupils should be taught how to use email positively and responsibly.

- Pupils may only use the email account linked to their Hwb account which is monitored by the Digital Lead
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers

Published content and the school website

The contact details on the website are the school address, email, Twitter account and telephone number. Staff or pupils' personal information will not be published. The Headteacher and Digital Lead will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing learner's images and work

- Images or videos that include pupils will be selected and used appropriately
- Parents must write to the Headteacher if they do NOT give permission for their child's photograph or work to appear online. Otherwise it is considered that consent has been given. This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where written consent will be required. Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the Ysgol Penyffordd website, or any other online accounts used by the school.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will insist that photographs/videos taken are of their own children only. Photos/videos that include images of other children must not be shared online unless permission has been granted from the parents of the other children.

Social networking and personal publishing

- The school will block access to certain social networking sites to pupils
- Pupils and parents will be advised that the use of many social network sites outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them and we will advise them on how to keep safe whilst using these sites.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the site/s before use.
- Learners are asked to report any incidents of cyberbullying to staff or an eCadet (who will then report to staff, who reports to the Child Protection Officer). All incidents are logged and log book can be found in safeguarding file
- School staff are strongly advised NOT to add past or present pupils as 'friends' if they use these sites
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. The school can also seek advice from the Police Liason Officer on these matters.

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and an informal risk assessment will be carried out before use in school is allowed
- Staff are encouraged to use cloud based storage rather than memory sticks to avoid loss of personal data related to staff or pupils. (See data protection policy)
- Pupils are strongly advised NOT to bring personal mobile devices/phones to school - unless there are exceptional circumstances. Any phones that are brought to school are handed in to the office and kept until the end of the day.

Information system security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be managed by Flintshire County Council
- Security strategies will be discussed with FCC
- Personal data taken off site must be secure saved in the cloud. All staff are responsible for the security of their portable digital storage and must report any losses or breaches to the Headteacher immediately.
- Files held on the school's network are subject to checks by members of the SMT.

Managing filtering

- Flintshire County Council provide a filtering service for all desktop computers and laptops. Filtering follows Welsh Government guidelines.
- Filtering systems will block all sites considered inappropriate • Changes to the school filtering policy will be risk assessed by the Headteacher and Digital Lead
- All breaches of filtering will be reported to the Digital Lead and the Headteacher if necessary. Staff and pupils are aware of this procedure
- The Digital Lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. We will work with the Flintshire County Council, and the internet service provider to ensure systems are effective to protect pupils.

Protecting personal data

See Data Protection Policy

Password Security

Staff are provided with an individual network and Flintshire County Council login username and password which can be accessed from all laptops and desktop computers. Staff and pupils also have individual Hwb accounts. Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the

security and confidentiality of the school network. Administrator passwords are controlled by Flintshire County Council on networks accessed via desktops and laptops. For all other systems administrator passwords are controlled by the Digital Leads.

Handling eSafety complaints

Complaints of internet misuse will be reported to the Digital Lead and/or Headteacher. All incidents will be logged and kept in the Safeguarding file, in the Headteachers office. Complaints of safeguarding must be dealt with in accordance with school safeguarding procedures. Pupils and parents complaints procedure can be viewed on our school website at www.ysgolpenyffordd.org

Monitoring and review

This policy, supported by the school's Acceptable Use Agreements/Code of Conducts, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT/Digital Learning, Home-school agreements, Behaviour, Safeguarding, and PSHE policies including Anti-bullying. Our eSafety policy has been written by the Digital Lead, building on advice from professional outside agencies and government guidance.

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Digital Lead. The adherence of this policy is the collective responsibility of the staff.

Policy approved by Head Teacher: Date:.....

Policy approved by Governing Body: (Chair of Governors) Date: