



## **Ysgol Bro Tawe**

### **E-Safety Policy**

The United Nations Convention on the Rights of the Child (UNCRC) is at the heart of our school's planning, policies, practice and ethos. As a rights-respecting school we not only teach about children's rights but also model rights and respect in all relationships. Our belief in "restorative approaches" ensures that every child is listened to.



Article 3: Everyone who works with children should always do what is best for each child.

Article 13: Your right to have information.

Article 19: you should not be harmed and should be looked after and kept safe.

### **Introduction**

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree with the school's approach to e-safety. The policy relates to other policies including ICT curriculum, Internet Access, Anti-Bullying, Child Protection and Health and Safety.

### **Writing and reviewing the e-Safety policy**

The school has a designated e-safety co-ordinator: Mrs Bethan Evans  
The e-Safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed on an annual basis.

### **Teaching and Learning**

#### **The importance of internet and digital communications**

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and learners.

It helps to prepare learners for their on-going career and personal development needs. At Ysgol Bro Tawe we believe that ICT is an essential life skill.

### **Internet use enhances learning**

Internet access is provided by Powys County Council and designed for pupils.

This includes filtering appropriate to the content and age of pupils.

Internet access is planned to enrich and extend learning activities.

Access levels are reviewed to reflect the curriculum requirement.

Pupils are given clear objectives for Internet use and sign an Internet agreement. Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Pupils are taught how to take responsibility for their own Internet access.

### **Pupils are taught how to evaluate Internet content**

Pupils are taught ways to validate information before accepting that it is necessarily accurate.

Pupils are taught to acknowledge the source of information, when using Internet material for their own use.

Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.

Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

### **Managing Internet Access**

#### **Information System Security**

School ICT system security is reviewed regularly.

Virus protection is updated regularly.

Security strategies are discussed with the Local Authority.

#### **E-mail**

Pupils are allowed to use Hwb e-mail accounts only.

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

In e-mails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.

Pupils are taught not to open suspicious incoming e-mail or attachments.

The forwarding of chain letters is not permitted.

#### **Published content and the school web site**

The website complies with the school's guidelines for publications.

Pupils are taught to consider the audience and purpose for the work they publish on the school website and ensure their work is of high quality.

All material must be the author's own work or where permission to reproduce has

been obtained, it is clearly marked with the copyright owner's name.  
The contact details on the website are for school admin only.

### **Publishing pupils' images and work**

Photographs must not identify individual pupils. Group shots or pictures taken "over the shoulder" are used in preference to individual "passport" style images. Children's photographs are only allowed to go on the website once written permission has been received from the child's parents. Children's photographs are not accompanied by names. Children's work which contains photographs must not also contain the child's name.

### **Managing filtering**

The school works in partnership with parents, the LA, The National Assembly for Wales, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

Senior staff ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

### **Managing video conferencing and webcam use**

Video conferencing is always appropriately supervised and pupils must ask permission before accepting or making any calls.

### **Managing emerging technologies**

Mobile phones must not be used during lessons.

Cameras in mobile phones or watches are not to be used by staff or pupils.

School cameras/ipads/tablets are used by both staff and children for educational purposes.

### **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

## **Policy Decisions**

### **Authorising Internet access**

Parents are asked to sign a consent form regarding their child's internet use.

### **Assessing risks**

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school, nor Powys LA can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

### **Handling e-safety complaints**

Complaints of internet misuse must be referred to 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 the school's child protection policy.

Pupils and parents are informed of the complaints procedure.

Pupils and parents are informed of the consequences for pupil misuse of the Internet.

### **Community use of the Internet**

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

## **Communications Policy**

### **Introducing the e-safety policy to pupils**

E-safety posters are posted next to all computers within classrooms and in a prominent place, so that all users can see them.

Pupils are informed that network and Internet use is monitored and appropriately followed up.

The children receive e-safety lessons including visits from the community police officer and are constantly reminded of online safety.

### **Staff and the e-safety policy**

All staff are trained regularly and receive a copy of the e-safety policy.

Staff are informed that network and Internet traffic can be traced to an individual user.

Staff will always use a child friendly safe search engine when accessing the web

with pupils.

### **Enlisting parents' and carers' support**

Parents' and carers' attention is drawn to the school's e-safety Policy in newsletters, the school prospectus and on the school website.

The school has links on its website to e-safety resources.

The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.