



Ysgol Gymraeg Dewi Sant

E Safety Policy

Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to Online Safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Child Protection and Health and Safety. The school has a designated Online Safety co-ordinator. The Online Safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed on a two year basis.

Date of original policy: 29/01/2025

Revised: 29/01/2027

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 students. It is a requirement of Curriculum for Wales and helps to prepare students for their on-going career and personal development needs.

Internet use Enhances Learning

Internet access is provided by Vale of Glamorgan 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 in KS2. Staff select websites 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.

Information System Security

- School ICT system security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the Local Authority

The learners' work is stored securely on the internal server and also via pupils' individual Hwb mail accounts. Work is also stored on apps approved by teachers e.g. Seesaw. On these occasions and in compliance with GDPR, parents are requested to give consent BEFORE pupils can gain

access. Learners are encouraged to think carefully about what they post on the app and to use kind words when evaluating the work of others. Accounts are monitored and reviewed regularly.

E-mail

Pupils are allowed to use Hwb email accounts only. Pupils must tell a teacher immediately if they receive an offensive or upsetting email or information. In emails, 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 email or attachments. The forwarding of chain letters is not permitted.

Published Content and the School Website

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

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. The staff are responsible for making sure that the pupils in the picture uploaded onto the school website have permission. A list will be compiled and updated regularly. Children's photographs are accompanied by first names only - Newsletters.

Social Networking and Personal Publishing

We do not use any type of chat rooms at this point. New applications will be thoroughly tested before pupils are given access. Please see our separate Instagram usage policy.

Managing Filtering

The school works in partnership with parents, the LEA, The National Assembly for Wales, Schoolmaster and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT coordinator.

Managing Video Conferencing and Webcam Use

Video conferencing uses the county approved program Visual Nexus and pupils must follow the school's Behaviour Policy. Video conferencing is always appropriately supervised and used during lessons.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit before use in school is allowed. Mobile phones are not to be used by pupils in school. If a pupil needs to bring a mobile phone to school it has to be handed in to the secretary/ Headteacher first thing in the morning for safe keeping. The teachers have a right to confiscate a mobile phone from any pupil. Cameras in mobile phones are not used by staff or pupils. Only school cameras are used by both staff and children for educational purposes. If visitors want to take pictures, they must have permission to do so.

Staff should not share personal telephone numbers with pupils and parents, unless they are personal friends. The school phone will be used for staff where contact with pupils is required.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access

All staff must read and sign the “Staff code of conduct for ICT” before using any school ICT source. The school maintains a record of all staff and children who have access to the school’s ICT systems. Parents are asked to sign a consent form regarding their child’s internet use (see Acceptable Use Policy).

Any person not directly employed by the school will be asked to read and sign the “acceptable use of school ICT resources” before being allowed to access the internet from the school site.

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 Vale of Glamorgan Council can accept liability for any material accessed, or any consequences of Internet access. The school’s Online Safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling Online 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 referred to the Senior Designated Professional or Deputy Designated Professional for safeguarding and dealt with in accordance with the school’s child protection procedures.

Pupils and parents are informed of the complaint’s procedure. Pupils and parents are informed of the consequences for pupil misuse of the Internet.

Pupils will be expected to follow codes of behaviour in virtual communications as well as face to face communications.

Community Use of the Internet

The school liaises with local organisations to establish a common approach to Online Safety.

Introducing the Online Safety Policy to Pupil

Online Safety posters are posted in school so that all users can see them. Pupils are informed that network and Internet use is monitored and appropriately followed up. The children receive Online Safety lessons and are constantly reminded of online safety.

Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils. The E-safety committee (Dreigiau Dewi Sant) will use the CEOP and Google Scheme to lead the learning of E-safety.

Staff and the Online Safety Policy

All staff are trained regularly and receive a copy of the Online Safety policy. Staff are informed that network and Internet traffic can be traced to an individual user. Discretion and professional conduct is essential.

Enlisting Parents' and Carers' Support

Parents' and carers' attention will be drawn to the school's Online Safety Policy in the school prospectus and on the school website.

The school has links on its website to Online Safety resources. Parents and carers will from time to time be provided with additional information on E-safety, especially during Safer Internet Day.

The school asks all new parents to sign the pupil/parent agreement when they register their child with the school. Parents have the right and opportunity to prevent their child from accessing the Internet at school.