



**Sully Primary School**  
**Ysgol Gynradd Sili**

# **E-Safety & Acceptable Use Policy**

Date of Ratification: January 2019  
Date of Review: January 2021

# **E-Safety Acceptable Use Policy**

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

Our e-safety policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

The e-safety policy and its implementation will be reviewed annually.

## **Teaching and Learning**

### Why internet use is important

The internet is an essential element in 21<sup>st</sup> 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.

### Using the Internet safely to enhance learning

The school's Internet access is filtered at source by our provider.

Activities that involve the use of the internet will be age appropriate.

Pupils using the Internet to search for information will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of keyword use, knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.

## **Managing Internet Access**

### Information system security

School ICT systems, capacity and security will be reviewed regularly in consultation with the school's Local Authority (LA) technician.

Virus protection will be updated regularly by the school's LA technician.

Security strategies will be discussed with the LA.

## E-mail

Pupils will be provisioned email addresses through the Hwb+ learning platform and taught about email through the school's ICT scheme of work.

Pupils may only access and use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive an offensive email.

Pupils must not reveal personal details about themselves or others via email or any other form of electronic communication. They must not arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper

Access to external personal e-mail accounts is not permitted.

The forwarding of chain letters is not permitted.

## **Social networking and personal publishing**

The school will not allow pupils or staff to access their personal social network sites. Newsgroups will be blocked unless a specific use is approved. Access to the school's Twitter account will be permitted to facilitate the sharing of work with the school's Twitter community.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils will be advised of the dangers of the use of social network spaces outside school

## **Managing Emerging Technologies**

Emerging technologies will be examined for educational benefit.

Pupils are not permitted to bring mobile phones into school without permission from an adult. If a mobile phone is brought into school then it must be kept by the office staff during the school day and will be made available for pupils to collect at home time.

## Protecting personal data

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

## **Policy Decisions**

### Authorising Internet access

All staff must read and sign the Acceptable ICT Use Agreement before using any school ICT resource.

Parents will be asked to sign a consent form granting permission for their child to use the internet.

The school will keep a record of all staff and pupils who's Internet access is restricted.

The record will be kept up-to-date, for instance a member of staff may leave or a pupils access be withdrawn.

At Foundation Phase, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

## **Assessing risks**

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

## **Handling e-safety complaints**

Complaints of Internet misuse will be dealt with by a senior member of staff.

Responses to Internet misuse may include informing parents/carers or removal of Internet/computer access for a set period

Any complaint about staff misuse must be referred to the Headteacher

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

## **Community use of the Internet**

The school will be sensitive to Internet related issues experienced by pupils outside of school, e.g. social networking sites. Appropriate advice and guidance on safe use will be given to pupils in Key Stage 2 via the curriculum and the school's Police Liaison officer.

## **Communications Policy**

### Introducing the e-safety policy to pupils

E-safety rules will be posted in the communal ICT area (Project Area) and in all KS2 classrooms and discussed with the pupils at the start of each year.

Pupils will be informed that Internet use will be monitored.

E-safety will be embedded in the ICT scheme of work and/or the PSHE curriculum. Specific e-safety lessons will be delivered via the school's e-safety curriculum. These lessons will be delivered from Year 1 to Year 6.

## **Rules for ICT Use**

1. We do not use offensive language, images, sounds and information
2. We tell an adult if we see anything we are uncomfortable with
3. We do not trespass into others' folders
4. We ask an adult before using a computer

### **Specific E-safety rules (Foundation Phase)**

- We only use the Internet when an adult is with us
- We click on the buttons or links when we know what they do
- We can search the Internet with an adult
- We always ask for help if we get lost on the Internet
- We can send or open emails together.
- We can write polite and friendly emails to people that we know.

### **Specific E-safety rules (Key Stage 2)**

- We ask permission before using the internet
- We do not use websites that look inappropriate
- We immediately close any web page we are not sure about and tell an adult
- We only e-mail people an adult has approved
- We send emails that are polite and friendly
- We never give out personal information or passwords
- We never arrange to meet anyone
- We do not open e-mails sent by anyone we don't know
- We do not use Internet chat rooms
- We ask for permission before posting messages on Internet forums

## **Media Publications**

Written permission from parents or carers will be obtained before photographs of pupils are published. The school will hold and administrate a list of pupil's names whose photograph is not to be shared or published.

Named images of pupils will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

The school website or VLE

The Local Authority web site

Hwb+

Web broadcasting

TV presentations

Newspapers

Twitter

Named pupil work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been provided.

## **Staff and the E-Safety policy**

All staff will be given the school's E-Safety policy and its importance will be explained.

Staff should be aware that Internet traffic can be monitored.

Discretion and professional conduct is essential.

## **Enlisting Parents' Support**

Parents' attention will be drawn to the school's E-safety Policy on the school's website.

A partnership approach will be encouraged. This could include demonstrations for parents/carers provided by the Community Police and discussions during Parent Forums.

## **Failure to Comply**

Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.