

E-Safety POLICY

Prepared: April 2016

Adopted: September 2016

Next Review: April 2019

**YSGOL GYMRAEG LLUNDAIN**

**LONDON WELSH SCHOOL**

**E-Safety Policy 2015 - 2018**

**Policy Review - 1st September 2018**

**Mission**

We strongly believe that our school has an integral role in keeping children safe in the community and when using technology. Our aim is to ensure that children can explore and develop their skills, knowledge and understanding to the fullest potential in a safe, nurturing and inclusive environment, which includes the wider community and on the internet. We offer the best possible provision and protection for all children in our care, with due regard to the evolving nature of technology.

**Compliance**

This policy complies with government guidance and advice on E-Safety *‘Advice on Child Internet Safety 1.0; Universal guidance for providers’ (DfE, UKCCIS, 2012)* and written with reference to the following documents:

* Disability Act 2010
* Equality Act 2010
* YG Anti-Bullying Policy
* YG Safeguarding Policy
* YG Accessibility Policy and Plan

**Definitions**

As outlined in the above document ‘E-Safety’ encompasses protection whilst operating the following within a school context, setting or wider community where appropriate;

* Internet Technologies e.g. e-mail, world wide web
* Electronic communications e.g. mobile phones

**Aims and Objectives**

We aim to provide simulative environments and access to technology within our school which is relevant to the child and the real world. This is to support children’s learning and with the outcome expected for children to be responsible and active members of the community. Technology offers a wide range of resources, information and knowledge which supports education and general administration systems on a daily basis. Whilst we acknowledge the beneficial use of technology in operating our school, we are aware of the continually developing nature of technology. We consequently strive to ensure our provision protects children and staff whilst operating technology, and that procedures are in place in the case of an incident or an at-risk situation, both inside and outside of school.

Our objectives to achieve are outlined below.

1. A designated teacher is appointed as the E-Safety Co-ordinator.
2. All teaching and non-teaching staff are aware and able to recognise e-safety issues
3. Offer provision of a recognised internet service provider (ISP) with age-related filtering
4. Established a clear reporting processes in the case of an incident
5. Support and advice offered to parents to ensure e-safety is a priority in school and at home.
6. Encourage open, honest and safe communication between pupils and staff to prevent any potential harm or risks. Such risks are made aware to parents, pupils and staff, with support networks available as needed.
7. Priority given to training, and continuation training, to all staff, including the contribution of the wider school community.

**Authorised Internet Access**

* All staff must read and sign the ‘Accepted ICT Use Agreement’ upon recruitment, and are aware before using any school ICT resource.
* Parents are informed upon pupil entry that they will be provided with supervised Internet access to enhance lessons and learning. They will be asked to sign and return a consent form for pupil access.
* Posters are displayed surrounding technological resources and equipment as a reminder of internet access guidelines and safe use of online use.
* Parental view restriction is in place on all laptops to restrict unauthorised and unsuitable websites.
* Provision of a recognised internet service provider (ISP) with age-related filtering is in place to restrict unauthorised and unsuitable websites.
* Should staff or pupils discover unsuitable sites, the URL address, time, content must be reported to the Designated E-Safety Officer.
* School will ensure that the use of Internet derived materials by pupils and staff complies with copyright laws.
* Pupils to be taught how to critically validate information online before accepting its accuracy, and to be aware of plagiarism when using.

**E-Mail**

* Pupils may only use approved e-mail accounts on the school system
* E-mails sent to external organisations from school email account must be written carefully and at times authorised before sending, in the same way as a headed letter.
* The sending of chain letters using school account is prohibited.

**Published Content**

* School website should contain school address, e-mail and telephone number but should not contain staff or pupil personal information
* Designated E-Safety teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
* Work and/or photographs which include pupils need to be carefully selected and comply with parental permission consent

**Social Networking**

* School filters may block access to social networking sites
* Care is needed when using the school social networking accounts that any post complies with permission consent from parents
* Pupils to be advised on personal details, photos and other identification information on their personal accounts and the consequent risks
* Pupils and staff to be advised on security and password safety.

**Information System Security**

* School ICT systems capacity and security will be reviewed regularly
* Virus protection will be installed and updated regularly

**Assessing Risks**

The school will take all reasonable precautions to prevent access to inappropriate material.

**E-Safety Incident**

The school will follow a rigorous procedure in the event of an E-Safety incident or at-risk situation is identified (e.g. access to unauthorised site is granted, cyber-bullying, risk of grooming).

**Storing and Managing Information**

Information and documents are stored in line with the government guidance under the Data Protection Act 1998 (DPA) on keeping and maintaining records. Please refer to ‘Gov.UK: Keeping and Maintaining Records’ for further information.

**Training and Resources**

Provision for the training is funded through the school’s central fund. As needed, training for staff is either provided within school or through the Local Educational Authority’s programme. Training aims to address the understanding and potential strategies and programmes to aid young learners.

**Complaints Procedure**

In the event of a complaint against the school, the processes within the Complaints Policy will be followed.

**Bullying**

Our ethos is to promote tolerance and independence in all our pupils. Further information is available in our Anti-Bullying policy.

**Other queries**

If you have any questions or queries about policy please contact the school directly.

Ysgol Gymraeg Llundain/ London Welsh School

Canolfan Gymunedol Hanwell Community Centre

Hanwell

W7 1PD

Tel: 020 8575 0237

Ebost/Email: info@ysgolgymraegllundain.co.uk

Appendices

# e-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

* The school owns the computer network and can set rules for its use.
* It is a criminal offence to use a computer or network for a purpose not permitted by the school.
* Irresponsible use may result in the loss of network or Internet access.
* Network access must be made via the user’s authorised account and password, which must not be given to any other person.
* All network and Internet use must be appropriate to education.
* Copyright and intellectual property rights must be respected.
* Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
* Anonymous messages and chain letters are not permitted.
* Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
* The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
* Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

|  |
| --- |
| **Ysgol Gymraeg Llundain E-Safety Rules**  **All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.**  |
| **Use of Images** As part of our everyday learning we will be using images and video for Learning Journeys, display, school website and school social media accounts. Only school equipment and resources (i.e. cameras, laptops) are to be used on site and to store images and videos, with exception to open and/or whole school events. On occasion the media may also use some of these images. If you do not wish your child to be included, please inform the school in writing.  |
| **Parent’s Consent for Web Publication of Work and Photographs** I agree that my son/daughter’s work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil’s full names. I have read and understood that I am giving permission for my child to be photographed at open school events. **Parent’s Consent for Internet Access** I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. |
| **Signed:**   | **Date:**   |
| **Please print name:**  |
| Please complete, sign and return to the school  |

Staff Information Systems Code of Conduct

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school’s e-safety policy for further information and clarification.**

* The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
* I will ensure that my information systems use will always be compatible with my professional role.
* I understand that school information systems may not be used for private purposes, without specific permission from the Lead Teacher.
* I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
* I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
* I will not install any software or hardware without permission.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
* I will respect copyright and intellectual property rights.
* I will report any incidents of concern regarding children’s safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
* I will ensure that any electronic communications with pupils are compatible with my professional role.
* I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school’s information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials 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 have read, understood and agree with the Information Systems Code of Conduct.**

Signed: ……………………………… Capitals: ……………………… Date: ………

|  |
| --- |
| Accepted for school: ……………………………. Capitals: ………………………….  |