Aim of Ysgol Gymraeg Gwynllyw
Providing excellent digital education for all children by fostering high aspirations and quality learning principles and discovering curiosity and exploration skills.
This Policy is linked to

- Child Protection Policy
- Protection Policy
- Anti-Bullying Policy
- ICT Policy
- GDPR

Principles

- Ysgol Gymraeg Gwynllyw is committed to providing a safe and secure environment for children, staff and visitors and promoting a climate where children and adults will feel confident to share any concerns they may have as a result of online safety issues.
- Gwynllyw recognizes the need to be alert to the risks of strangers or others (including parents or carers of other students) who may wish to harm children at school and will take all reasonable steps to reduce such risks by promoting e- safety. and acceptable use policies that everyone clearly understands and respects.
- The policy applies to all on-site and off-site activities carried out by students while they are the responsibility of the school.

Purposes

- Outline the nature of e-safety and how staff and students can recognize it.
- Identify simple ways in which e-safety can be reported to responsible adults.
- Provide clear policy and guidelines to enable e-security to be tackled effectively.

The E-Safety leader in the School will work alongside the Designated Child Safeguarding Officer.
Guidelines

Why the internet and digital communication is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide high quality internet access for pupils as part of their learning experience.
- Using the internet is part of the statutory curriculum and is a necessary learning tool for staff and students.

Using the internet will enrich and extend the learning

- Staff will be informed about using the internet safely and students will be taught
- Clear boundaries will be set and discussed with staff and students, for appropriate use of the internet and digital communication.
- Students will be taught to use the Internet effectively in research, including skills in locating, retrieving and evaluating information.

Students will be taught how to evaluate Internet content

- The school will ensure that the use of materials derived from the internet by staff and students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to verify information before accepting its accuracy.

Internet Access Control

Information system security

- The security of the school's ICT system will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- SRS will regularly monitor all activities.
- Any potential breaches of security will be reported to the Headteacher or nominated ICT leader who will report to SRS and the Local Authority immediately and deal with it accordingly.
- Breaches of GDPR resulting from online activity will be dealt with in accordance with the GDPR policy.

E-bost

- Students and staff should only use approved curriculum email accounts. (Outlook account and staff G-mail and student G-mail)
- Students must be aware of how they can report abuse and to whom they should report abuse.
- Students must report any email they receive to a member of staff.
- In email communications, students should not disclose their personal or other personal details, or arrange to meet anyone without specific permission.
- Incoming emails should be treated as suspicious and attachments should not be opened unless the author is known.
- The school should consider recommending a standard post format for all users.
- Forwarding of chain letters / emails is not allowed.
- Staff must use a school email for electronic communication regarding school business.
- The use of the school email is for professional use only.
- Staff must follow additional steps to ensure that sensitive data is secure when sending information by post.

School website

- Personal contact information of staff or students will not normally be published. The contact details given online should be the email addresses of the school office or designated school staff.
- The Headteacher or nominee will take overall editorial responsibility and ensure that the published content is correct and appropriate.

Published content and Digital Learning Platforms

- Private and personal contact information of staff or contact persons will not be published. The details provided will be the individual's official curriculum email address.
- Images, comments and personal files will not be published by pupils or staff.
- All members of staff have a responsibility to ensure appropriate use of their Google Classroom and to report any misuse to the safeguarding leader.

Publishing images and student work

- Photographs containing students will be carefully selected so that individual images are not misused
- Students' full names are not used anywhere on the school's websites or any other online space, especially in connection with photographs.
- Written consent, using the approved consent form, is requested from parents or carers before publishing pictures of students on the Websites/VLE.
- Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

- The school will educate people to use social networking sites safely, and educate students to use them safely. Students are advised never to give personal details of any kind that could reveal who they are, their friends or their location.
- Students must be aware of how they can report abuse and to whom they should report abuse.
- The students should be taught why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to prevent access to unknown individuals and to block unwanted communications. Students should only invite known friends and refuse entry to others.
- Staff are advised not to run personal social network spaces for student use.
- Staff are advised not to include work-related contacts (parents, pupils or former pupils) on their personal social media.
- It is forbidden to discuss issues/information related to work by staff, on a social network site, and it would become a disciplinary matter for those who break this principle.
- Staff may not upload school images of pupils on their personal social media, and it would become a disciplinary matter for those who breach this principle.

- Staff must be aware that information stored, displayed or discussed on networking sites is public.
- Parents, pupils and staff should be aware that bullying can happen through social networking sites. (See section below)

Manage monitoring and filtering

- Senior staff will ensure that regular checks are carried out to ensure that the filtering methods chosen are appropriate, effective and reasonable.
- If staff or pupils find an unsuitable site, the E-Safety Leader or Network Manager must be informed.
- Logs of internet outages are kept and reviewed. Access to any illegal, questionable websites will be reported to the appropriate agencies.

Manage video conferencing / VLE

- Students should seek permission from the supervising teacher before making or answering a video conference call.
- Google Suite settings should ensure that only the teacher can initiate a conference call through Google Classroom.
- Video conferencing will be supervised appropriately for the age of the students.
- Teachers will receive permission from parents and guardians before children can participate in video conferences with the school.
- Staff will establish a dialogue with other conference participants to assess the risk, before participating in a video conference. If it is not a school site, it is important to check that they distribute material that is suitable for the class.

Management of technologies

- New technologies will be examined for educational benefit and a risk assessment will be carried out before they are allowed to be used in the school.
- The governing body and senior leaders are aware that technologies such as mobile phones with wireless internet access can bypass schools' filtering systems and present a new route to objectionable material and communication.
- Where it is necessary to contact Students to facilitate their learning, staff will be given a school phone or dial 141 in order to block their contact number.
- Sending offensive or inappropriate text messages is prohibited.
- Student use of cameras in mobile phones will be continuously reviewed.
- In the primary sector, mobile phones are not allowed to be used during lessons or formal school time.
- It should be noted that gaming machines including the Sony Playstation, Microsoft Xbox and others have internet access which may not include filtering. Care is required in any use at school or other officially permitted location.

Protection of personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.
- Data containing sensitive information, be it personal or work related information eg documents will be encrypted, this applies when data is on a hard drive and personal data should not be stored on a portable storage device .
- Personal or sensitive data should be deleted when it is no longer needed.
- Any personal or financial data transmitted electronically should be encrypted or password protected.

Policy Decisions

Authorize access to the Internet

- All members of staff and visitors must read and sign the 'Staff and Code of Conduct for ICT' before using any school ICT resource, including any laptop given for professional use.
- The schools will keep an up-to-date record of all the staff and students who are allowed to use the school's ICT systems.
- Secondary age students must apply for Internet access individually by agreeing to comply with the Responsible Use of the Internet statement in the school's Acceptable Use Policy.
- All users using personal devices must sign and agree to the 'Bring Your Own Device' (BYOD) Policy as set out by SRS.

Assess risks

Dealing with e-safety complaints

- There will be complaints for misuse of the Internet are reported to the e-safety lead.
- Any abuse by staff that suggests a crime has been committed, a child has been harmed or that a member of staff is unfit to work with children should be reported to the LA within one working day in accordance with Protection policies.
- Any complaint about abusive staff should be referred to the Headteacher or the Safeguarding Leader and if it is the Headteacher who is the abuser, it must be referred to the Designated Safeguarding Governor.
- Students, parents and staff will be informed of the complaints procedure.
- The school and SRS will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and connected nature of Internet content, it is not possible to guarantee that inappropriate material will never appear on a computer connected to a school network The school accepts no responsibility for any material accessed, or for any consequences of access to the Internet.
- The school and SRS should examine the use of ICT to establish whether the E-Safety policy is sufficient and that the implementation of the E-Safety policy is appropriate and effective. The school will ensure that appropriate monitoring software and procedures are in place.

E-Safety Communications

Present the E-safety policy to students

- E-safety rules will be posted in all rooms where computers are used. All users of the system will be informed that use of the network and the Internet will be monitored.
- A program of E-Safety training and awareness raising will be implemented as part of the pastoral programme.
- In the primary sector, an e-safety module will be included in all parts of the curriculum, particularly in PSE and Computer Science study programmes, which cover school and home use in accordance with the Curriculum for Wales.

Staff and the E-Security Policy

- All staff will have access to the school's E-Security Policy and its importance will be explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- Staff who manage filtering systems or monitor the use of ICT will be supervised by senior leaders and work to clear procedures for reporting issues.
- Staff should understand that communicating by phone or online with students can occasionally lead to misunderstandings or even malicious accusations. Staff must always take care to maintain a professional relationship.
- Training is provided to staff in safe and responsible use of the Internet and on the school's E-safety Policy as required.

Enlist the support of parents and carers

- The attention of parents and carers is drawn to the school's E-Safety Policy in newsletters and on the school's website and the school's website.
- The school will keep a list of E-safety resources for parents/carers on the school website.

The Current Situation

An e-safety policy is in place and the school has shared it on the School's website. As a result of significant changes in the way technology is used since March 2019, this policy needs to be regularly updated and our e-safety program needs to be added to raise awareness among pupils, staff and the wider community. An acceptable use policy is in place and is accepted by staff when logging into the school's systems.

The new curriculum and HWB guidelines that use 360SafeCymru provide clear and specific guidance on how to ensure that policies and procedures are sound and safe. With the support of SRS and Torfaen, security measures are in place to protect against GDPR breaches and in the event of scamming, phishing and hacking.

An audit has been completed using the 360SafeCymru online tool and progress is needed to make changes to policies and the curriculum.

The Next Steps

- Mark Jones (Support Head), Rhian Dickenson (Assistant Head) and Rhian James (Safeguarding Leader) will work together to ensure that sufficient training is received.
- A comprehensive program of education and training for pupils and staff will be coordinated to meet statutory requirements in terms of e-security.
- Policies and Procedures will be updated and presented to the Governing Body by the end of this academic year.
- A 360Wales audit will be completed regularly to ensure that progress is made and shared with the Governing Body.

This policy has been agreed by the Governing Body and will form part of the school's digital strategy.

Signed:

Headteacher	Chair of Governors
Mark Jones	Lesley Bush
27.9.23	27.9.23

Updated: 10.5.23