Dogfen Polisi | Policy Document

e-ddiogelwch
e-safety

Ysgol Gymraeg Gilfach Fargod

Adopted By	Governing Body (Ysgol Gymraeg Gilfach Fargod)
Dyddiad Mabwysiadu / Adoption Date	Mai 2023 / May 2023
Dyddiad Adolygu / Review Date	Mai 2025 / May 2025

Mae polisïau Ysgol Gymraeg Gilfach Fargod ar gael i holl rhanddeiliaid yr ysgol eu gweld ar unrhyw adeg.

Ysgol Gymraeg Gilfach Fargod's policies are available for all school stakeholders to view at any time.

Ysgol Gymraeg Gilfach Fargod
Pennaeth: Mr. Jamie Hallett | Dirprwy Bennaeth: Mr. Aled Hopton
Ffôn: 01443 875528 | E-bost: ygbpa@caerphilly.gov.uk | Trydar: @yggf123

Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by the Ysgol Gymraeg Gilfach Fargod e-Safety Group made up of:

- ★ Deputy Headteacher
- ★ e-Safety Coordinator
- ★ Teachers and Teaching Assistants
- ★ E-Safety Governor
- ★ Parents
- ★ Pupils

Schedule for Development/Monitoring/Review

This e-Safety policy was approved by the Governing Body on:	
The implementation of this e-Safety policy will be monitored by the:	Senior Leaders e-Safety Coordinator e-Safety Group
Monitoring will take place at regular intervals:	e-Safety Group will meet termly
The Governing Body will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	Caerphilly Borough County Council's Safeguarding Team.

The school will monitor the impact of the policy using:

- ★ Logs of reported incidents
- ★ Surveys / questionnaires of
  - students / pupils
  - parents / carers

- staff

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school :

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor to include:

- ★ regular meetings with the e-Safety Coordinator
- ★ regular monitoring of e-Safety incident logs
- ★ reporting to relevant Governors / sub-committee / meeting

Headteacher:

The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community.

- ★ The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- ★ The Headteacher will receive regular monitoring reports from the e-Safety Coordinator.

e-Safety Coordinator:

Will:

- ★ lead the e-Safety committee
- ★ take day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ★ ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- ★ provide (or identifies sources of) training and advice for staff and pupils
- ★ liaise with LA technical staff
- ★ receive reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- ★ report regularly to Senior Leadership Team

Caerphilly County Borough Council

Will ensure:

- ★ that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ★ that users can only access the networks and devices by use of controlled logins and passwords.

Teaching and Support Staff

Are responsible for ensuring that:

- ★ they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- ★ they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- ★ they report any suspected misuse or problem to the Headteacher / e-Safety Coordinator for investigation / action
- ★ all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- ★ they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Safeguarding Designated Person

The Safeguarding Designated Person should be trained in e-Safety issues and be aware of the potential for serious safeguarding issues to arise from:

- ★ sharing of personal data
- ★ access to illegal / inappropriate materials
- ★ inappropriate online contact with adults / strangers
- ★ potential or actual incidents of grooming
- ★ cyber-bullying

e-Safety Group

The e-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and monitoring the e-Safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the e-Safety Coordinator with:

- ★ the production/review/monitoring of the school e-Safety policy/documents;
- ★ consulting stakeholders – including parents/carers and the students/pupils about the e-Safety provision;
- ★ monitoring improvement actions identified through use of the 360 Degree Safe Cymru self review tool.

Students/pupils:

- ★ are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- ★ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- ★ will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- ★ should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- ★ endorsing (by signature) the Pupil Acceptable Use Agreement
- ★ agree (by signature) to the conditions outlined in the Parent/ Carer Acceptable Use Agreement
- ★ accessing the school ICT systems or learning platforms in accordance with the school Acceptable Use Policy.

e-Safety Education

Pupils

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- ★ Planned e-Safety lessons should be provided as part of the Welfare / ICT lessons or other lessons and should be regularly revisited
- ★ Key e-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- ★ Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- ★ Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Parents/carers

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- ★ Curriculum activities
- ★ Letters, newsletters, web site
- ★ Parents / Carers evenings / sessions
- ★ High profile events / campaigns eg Safer Internet Day
- ★ Reference to relevant websites

Staff

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- ★ A programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly.
- ★ All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.

Governors

Governors should take part in e-Safety training / awareness sessions. This may be offered in a number of ways:

- ★ Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- ★ Training provided for the Governors by the e-Safety Coordinator.

Technical - infrastructure / equipment, filtering and monitoring

- ★ Caerphilly County Borough Council uses web-filtering software to control access to websites and pages and to monitor user activity. The software will block access to websites, pages or content that is inappropriate or not relevant to the business of the Council. Web Filtering policies are applied in line with Welsh Government Guidelines.
- ★ To address the security risks posed by having access to the Internet the Council has a number of security Controls such as Anti-Virus applications, Firewalls and Web-filtering software in place to protect its network and information systems.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- ★ When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- ★ In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- ★ Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes without express permission from the Headteacher.
- ★ Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- ★ Photographs published on the website, or elsewhere, that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
  Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ★ Permission from parents or carers will be obtained through the Home-School Contract before photographs of students / pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- ★ Fairly and lawfully processed
- ★ Processed for limited purposes
- ★ Adequate, relevant and not excessive
- ★ Accurate
- ★ Kept no longer than is necessary
- ★ Processed in accordance with the data subject's rights
- ★ Secure
- ★ Only transferred to others with adequate protection.

The school must ensure that:

- ★ It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- ★ Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- ★ All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- ★ It has a Data Protection Policy
- ★ It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- ★ At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- ★ Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" of their Google account (or other account which holds personal data e.g. Hwb) and the computer at the end of any session in which they are using personal data.
- ★ Transfer data using encryption and secure password protected devices.
- ★ Keep their computer login and logins for online accounts which hold personal data (e.g. Google, Hwb) private.

Personal data should not be stored on any memory stick or any other removable media.

The school is aware that changes to Data Protection laws will come into force in 2018 under the General Data Protection Regulation, and are actively preparing for these changes. This policy will be reviewed and, if necessary, amended to reflect the new laws as soon as possible.

Communications

When using communication technologies the school considers the following as good practice:

- ★ The official school email services (@caerphilly.gov.uk, @caerphilly.org.uk and @hwbmail.net) and may be regarded as safe and secure. Users should be aware that email communications are monitored.
- ★ Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- ★ Any digital communication between staff and students / pupils or parents / carers (email, Schoop, etc) that relate to school matters must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications unless specific permission has been granted by the Headteacher.
- ★ Personal information should not be posted on the school website, other than names (first name only for pupils) and only official email addresses should be used for members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- ★ Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- ★ Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- ★ No reference should be made on social media to students / pupils, parents / carers or school staff
- ★ They do not engage in online discussion on personal matters relating to members of the school community
- ★ Personal opinions should not be attributed to the school or local authority
- ★ Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's official use of social media for professional purposes will be checked regularly by the e-Safety committee to ensure compliance with school policies.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, report immediately to the police.

Inappropriate Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. We refer to these activities as Inappropriate activities, and they include the following:

pornography, promotion of any kind of discrimination, threatening behaviour, including promotion of physical violence or mental harm, any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute, using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school, revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords), creating or propagating computer viruses or other harmful files.

It is important that any inappropriate actions are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Such incidents will be dealt with through normal behaviour / disciplinary procedures.