

Caban Y Faenol CYF

Internet Safety

The internet is part of everyday life. Knowledge and experience of technology should be considered as essential. Developmentally appropriate access to the internet in the early years contributes significantly to children's learning and their management of their learning experiences, but there is a level of risk attached to this. Children should be aware of the possible dangers of online technologies in order to empower them with the knowledge and skills to keep safe, without restricting their learning opportunities and experiences.

The setting endeavours, insofar as it is able, to support the children's learning experiences through the use of a range of Information and Communication Technologies (ICT) resources, and also to enable the setting's practitioners to use a range of ICT resources to support their work.

The Internet Safety Policy aims to provide advice on acceptable use and effective measures to enable children and adults to use the internet in a safe way.

This Policy is applicable to everyone who has access to/uses the setting's internet connection. This includes children, parents/carers, practitioners and their managers, volunteers, students, committee members, visitors, contractors, and members of the community. This list is not exhaustive. It is also applicable if the setting uses the landlord's internet access, e.g., in a village hall or school. It applies to every device with internet access, including computers, smart phones, tablet computers or mobile gaming devices.

The Rights of the Child

Ensuring safe use of digital technology is part of ensuring that the Cylch Meithrin respects the rights of the child, as noted by the United Nations Convention on the Rights of the Child, specifically:

- Article 3: All organisations concerned with children should work towards what is best for each child.
- Article 16: Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.
- Article 19: Governments should ensure that children are properly cared for, and protect them from violence, abuse and neglect by their parents or anyone else who looks after them.
- Article 28: Children have a right to an education. Discipline in schools should respect children's human dignity. Primary education should be free. Wealthier countries should help poorer countries to achieve this.
- Article 31: All children have a right to relax and play, and to join in a wide range of activities.
- Article 34: Government should protect children from sexual abuse.

Caban Y Faenol CYF

Article 36: Children should be protected from any activities that could harm their development.

The person responsible for child safeguarding is responsible for day-to-day online safety and for implementing the Internet Safety Policy. They will ensure that all web users are aware of this policy, and that effective training and online safety advice is provided, and that it is available to them – this includes advice and support for children and parents/carers, as required.

A full list of responsibilities is available in the Guidelines: Online safety for early years practitioners support pack [38689 \(gov.wales\)](#)

The setting meets with statutory requirements to ensure that children are safe and protected from possible abuse, including online abuse. Practitioners are aware of the possible dangers to children, practitioners, and parents/carers.

Acceptable Use Agreement

The aim of the Acceptable Use Agreement is to:

- protect children through appropriate and acceptable use of technology.
- Outline the responsibilities of everyone who has access to technology systems in their workplace.
- Ensure that everyone is aware of the dangers, understands what constitutes misuse, strategies for misuse and responsible use.

Acceptable use by practitioners, their managers , and volunteers

The authorisation of the person responsible for child safeguarding within the setting enables practitioners, their managers and volunteers to use online technologies in their work.

This Internet Safety Policy will be presented as part of the induction process for new practitioners, and they must sign to confirm that they have read and understood the policy.

Acceptable use by parents/carers/guardians

As laid out in our Data Protection Policy, we will ask parents to support the setting's good practice by following our guidelines when taking and sharing of photos of the setting's activities, e.g., sports day, Christmas concert, on social networking sites. This policy states that no images/recordings/videos etc. taken in the setting/of children, staff, volunteers and other service users/suppliers may be published in any way.

Acceptable use by children

Caban Y Faenol CYF

We will use Acceptable Use Agreements to help children and their families to understand the behaviour expected of them when using the internet. We will share this with children in an age-appropriate way, for example, through pictures, posters, or discussion activities, and by talking with the parents/ carers of the youngest children. We will encourage parents/ carers to agree to help their child understand what is acceptable/ unacceptable online, especially with the youngest children.

Acceptable Use Agreements are shared with and agreed upon by the children and are displayed prominently in the setting to remind them.

At Caban Y Faenol we offer children the opportunity to use the computer and the internet, however we have introduced a range of procedures to ensure their safety. These measures are as follows:

- As we are linked to the school internet provider there is a filter on each computer that blocks out most inappropriate material
- We do not permit the children to go onto chat rooms
- We talk to the children about the websites they are using
- We are always nearby so can keep an eye out on what websites they are visiting
- We check the history on the computer regularly
- We discuss with the children about the importance of keeping safe on line, not forwarding on chain letters, not talking to people they don't know, not giving out personal information that could enable people to identify them.
- We encourage them to tell a member of staff if they are worried about anything they have seen/said/been told online
- We emphasise that they never arrange to meet anyone they have spoken to online.
- When completing the registration form there is a box for parents to tick that gives their permission for their child to access the internet.
- During after school club children are limited to 15 minutes per session on the computer.
- During holiday club they will be allowed a slot in the morning, after lunch and late afternoon.

The rules above also apply when children are using other devices to gain internet access such as laptops and ipads.

Acceptable use by visitors, contractors and others

Any visitors or contractors must adhere to all guidelines on the acceptable use of technology.

The setting commits to ensuring that personal data will be stored, processed, and transferred according to the Data Protection Act/ GDPR 2018 by ensuring that personal data is handled in a way that:

- is fair and transparent
- ensures it is processed for limited purposes

Caban Y Faenol CYF

- is sufficient, relevant and not excessive
- is accurate
- ensures it is stored for the least amount of time possible
- ensures it is processed in accordance with the individual's rights
- ensures safe storage
- ensures that it is only transferred to others with sufficient protections in place

See the setting's **Confidentiality and Data Protection** Policy for full details.

Cloud Computing

Cloud computing is a term describing the use of technological services - such as email, document storage, or software – over a network such as the internet. One of the advantages of cloud computing is the ability to access these services from a variety of locations, and that various users all have access (e.g., payments being updated by the leader in the setting, and the treasurer working from home to complete the setting's accounts).

The setting acknowledges that there are advantages to using Cloud Computing systems. We are also considerate of the fact that practitioners have a duty of care over the setting's children. The setting commits to offering opportunities to develop appropriate and safe use of this technology for the benefit of practitioners and the children.

The setting commits to storing any data on the Cloud Computing system in line with the requirements of the Data Protection Act 1998.

The setting will:

- ensure that only the setting's practitioners/committee have the passwords to access the cloud storage¹.
- clearly note who among the setting's practitioners/ committee/ managers have access to passwords, and formally record who is given the passwords during official meetings (e.g. committee meetings), noting the decision in the minutes of the committee meeting.
- ensure that a password is needed for access to digital documents storing sensitive information.
- ensure that all users of the cloud data storage system have a unique username and password.
- add to, update the rights of, and delete individual accounts in a timely fashion; for example, when a member of staff ceases to work at the setting, once a new staff member begins in the setting, or when there is a new chairman for the committee.

Caban Y Faenol CYF

- expect authorised users to ensure that antivirus software and firewalls are up to date and operational on any devices used to access the cloud storage system.

Keeping passwords safe

The setting ensures that passwords are stored safely by following the measures outlined in the password guidelines.

The setting will:

- ensure that a password is required to gain access to digital equipment storing sensitive information.
- ensure that only the setting's **practitioners/ committee/ managers** have access to passwords, and clearly note who is given the passwords during official meetings (e.g. committee meetings), recording the decision in the minutes of the committee meeting.
- ensure that practitioners are all responsible for keeping their passwords safe and updating them regularly, and that everybody has a strong password.
- set a time limit for each session's length on every device with access to the web.
- ensure that every user in the provision signs out of their account if they leave a device.
- If a user thinks that the security of their password has been compromised, or the password was shared, intentionally or unintentionally, then they will report the concern to the person responsible for child safeguarding
- change the password on devices if a member of staff leaves.

If personal data is stored on any portable digital devices, the setting will:

- ensure that the portable digital device is password protected.
- ensure that the data is password protected.

Access to the internet

The setting manages internet access by keeping to the measures outlined in the Web Access guidelines.

The setting will put measures in place to manage access to the web and reduce risks, including:

- secure broadband or Wi-Fi access.
- secure e-mail accounts.

Caban Y Faenol CYF

- an antivirus system which is regularly monitored and updated.
- a safe password system.
- an agreed list of authorised users with managed access and defined responsibilities.
- clear acceptable use agreements.
- effective inspection, monitoring and reviewing procedures, e.g., monitoring that staff do not connect to the internet from their personal phones, that staff are not using the setting's equipment to access the internet e.g. during their lunch hour, monitor which sites staff are visiting.
- parental controls on equipment such as computers and iPads.
- ensuring that each staff member is aware of their responsibility to supervise children whilst they are using digital technology.
- expecting practitioners to verify the suitability of any website, games, or apps they intend to use with the children beforehand, and regularly after the first use.
- use age-appropriate software to develop the children's skills and knowledge.
- locating devices which have access to the internet in visible areas and supervising adults and children closely and monitoring their online usage appropriately.
- making all practitioners aware of the dangers of connecting mobile personal devices to work systems.
- where required, ensure that any files or programs downloaded to work systems are effectively monitored and managed.
- Report any concerns arising from the use of online technologies to the person responsible for child safeguarding.

Online communications

When communicating online, the setting will keep to the measures outlined in the Online Communications guidelines.

E-mail

The setting will:

- clearly note who (e.g. **practitioner/ volunteer/ manager/ committee member**) may send communications on behalf of the setting, e.g. in an official meeting (e.g. committee meeting or management meeting), and that this decision is recorded.

Caban Y Faenol CYF

- expect practitioners to use only the setting's email account for the setting's official business, including communicating with parents and carers.
- expect practitioners not to send or receive personal communications using the setting's official email account.
- expect practitioners not to send unauthorised emails on behalf of other individuals.
- remind parents/ carers and practitioners about the Compliments and Complaints Policy procedure to ensure that any complaint is directly referred to the setting's **Committee/ Registered Person/ Responsible Individual**.
- use secure, filtered email accounts.
- be aware that online email services are not considered safe for personal data, and that using them may pose a risk to us. We will therefore avoid sending personal data over email where possible. If we are unable to avoid sending personal data over email, we will secure the personal data with our own systems, for example password protection or encryption, or by using the data protection systems of the agency that has requested the personal data. It is more secure for us to receive personal data on paper, but when parents/ carers/ agencies send us personal data via email, it is their responsibility to protect that data.
- inspect and monitor every email communication.
- communicate online in a polite and respectful manner, without using any insulting language.
- encourage the appropriate use of profile pictures.
- operate within legal requirements, for example laws/ data protection policy, and in line with policies.
- contact children for professional reasons only, and do so carefully in order to avoid any misinterpretation.
- avoid sharing any of the children's personal information/ details.
- do not ask for, nor respond to any personal information from a child unless it is appropriate to do so as part of the professional role, or if the child is in direct danger of being harmed.
- use appropriate reporting pathways should we suspect that personal data has been released.
- ensure that practitioners are aware of the strategies for responding to misuse, which can be followed if policy is breached.

Caban Y Faenol CYF

- not open emails if we do not recognize the sender/ if the format looks suspicious, and be exceptionally careful when opening any attachment.

Misuse of information and communication technology guidelines

In an instance where information and communication technology is being misused, the setting will follow the steps outlined in the Misuse of Information and Communication Technology guidelines.

Parents/ carers and other agencies, if relevant, will be informed of any incident where technology was inappropriately used within the provision, and if relevant, outside of the provision.

The setting will:

- ensure that relevant online safety policies and procedures are implemented, monitored and reviewed fully, that they are thorough, convenient and reflect practice, and that they are shared with all users of the provision.
- inform users of possible signs of any misuse in order to identify any significant changes as quickly as possible.
- inform users that misuse of technology and/or breaching relevant policies and procedures is a serious matter, and that the strategies implemented in response to misuse and definitions of responsible use are clearly defined and can be implemented if concerns arise.
- ensure that effective procedures for reporting and whistle-blowing are in place and that they are promoted.

Procedure in case of a misuse of information and communication technology

The setting will:

- deal with incidents one case at a time.
- ensure that context, intent and effect are considered when deciding upon the response and the steps to take. For example, a series of small incidents by an individual might be treated differently to a single incident. Intentional and unintentional access to inappropriate websites would bring about different levels of intervention and response.
- record and monitor every online safety incident, identifying any possible behavioural patterns, in order to be able to respond proactively and safeguard the relevant individuals.
- report the incident to the person responsible for child safeguarding
- make a written record of the incident and monitor the situation. See Appendix 3

Caban Y Faenol CYF

- in cases when an inappropriate website was unknowingly accessed, the setting will add it to the list of banned or restricted websites which is set using filter settings.
- report - an open reporting policy is in place, which means that any instances when the policy was unintentionally breached, or any access to inappropriate material, is reported. Failure to report breaches of policy such as these will lead to the concern being referred upwards.

Serious incidents

The setting will:

- deal with every serious incident immediately and report at once to the person responsible for child safeguarding
- consider the context, intent and effect of the alleged misuse.
- take appropriate steps, as agreed upon by the person responsible for child safeguarding and the relevant senior manager.
- record the details clearly and legibly.
- record the reason for any decision taken.
- follow the provision's Child Safeguarding Policy if a child has been abused or is being abused.
- refer the case upwards by following the local child safeguarding procedure or contact the police or children's social care services, if relevant.
- follow the setting's Child Safeguarding Policy immediately if the incident pertains to an accusation made against a member of staff, manager, volunteer or student, and there is the suggestion that the child has been abused in any way. In the case of an accusation being made against an adult, the local authority must be informed, as well as the police and Care Inspectorate Wales (if relevant).
- not conduct an investigation or internal interview in connection with an accusation, unless an investigative agency has asked us specifically to do so. If an accusation of abuse is made, the police, children's social services and/ or the local authority will conduct the investigation.
- secure any device or hardware as evidence if it may be relevant to any possible investigation of abuse. We will not follow internal disciplinary procedures until all investigations by relevant agencies have been completed.
- ask for advice from human resources or legal advice before conducting any internal investigation and/ or conducting any high level disciplinary.

Caban Y Faenol CYF

- conduct a review of online safety after the completion of internal and external investigations, or sooner if appropriate to do so. Revise and update policies and procedures as required.
- consult with all the provisions users, if relevant, on any revisions likely to be made.
- distribute the revised policies and procedures as appropriate.

We will report the following incidents to the police each time, and (if relevant) contact child safeguarding services, children's social services, the local authority and Care Inspectorate Wales (CIW):

- the discovery of indecent images or videos of children and young people
- behavior which is considered to be 'fostering an inappropriate online relationship'
- the sending of indecent materials
- attempts to radicalize or share extremist views

Failure to report these incidents may result in an offence being committed.

- We will make no effort to download print or send any materials we may find. Doing so may be carrying out a further offence.
- if materials which may be illegal are discovered we will avoid, as far as practically reasonable, touching any of the equipment nor materials.
- neither delete nor forward the contents.
- secure the device and store the passwords/ access rights until they are passed to the police.
- not switch off the devices unless the police authorize us to do so.
- restrict further access to the illegal contents by keeping individuals away from the area in question.
- report to the Internet watch Foundation 34, giving details of the web address, if there has been online access to image (s) or video (s) of sexual child abuse which may be illegal.
- report the concern as a matter of caution, if we are unclear as to whether it is illegal or not.

If a child misuses technology

It is unlikely that a child in the setting will intentionally misuse technology. Should this happen, we will consider it a safeguarding concern and will follow the usual safeguarding procedures.

We will:

Caban Y Faenol CYF

- follow the Misuse of Information and Communication Technology Guidelines in this policy.
- inform the parent/ carer of the matter.
- discuss with the child how and why this happened, giving consideration to the child's age and any additional needs they may have.
- give the child support and guidance.

If a child accidentally obtains inappropriate materials, they must report the matter immediately to an adult. We will take appropriate steps to hide or minimize the window. We will not switch off the device nor close the page, in order to be able to investigate the matter. We will talk with the child and their parent/ carer. We will take appropriate steps following the incident to ensure that it does not take place again in the future.

Media attention

Should an incident attract attention and speculation from the press, the setting will make every possible effort to ensure that children, practitioners and parents/ carers are protected and appropriately supported. We will implement any major strategy and only authorised practitioners will release statements, in line with information sharing procedures. In every case our main concern will be safeguarding children and the well-being of children and their families. We will ask for support from our Support Officer before engaging with the media.

Misuse of information and communication technology may lead to disciplinary action and a serious case may lead to dismissal in line with the setting's disciplinary procedure. (See staffing policy)

Guidelines and a record reviewing internet sites are available on HWB:

[Repository - Hwb \(gov.wales\)](https://gov.wales/repository)

Contacts and useful information

We recommend referring to the publications and websites below for more information:

A full list of responsibilities is available in the Guidelines: Online safety for early years practitioners support pack [38689 \(gov.wales\)](https://gov.wales/38689)

Hwb's Keep Safe Online Section: hwb.llyw.cymru/cadwnddiogelarlein

Child Exploitation and Online Protection Centre: <https://ceop.police.uk/safety-centre/>

Caban Y Faenol CYF

The UK Centre for Safer Internet Use:
www.saferinternet.org.uk

UK Council for Internet Safety: www.gov.uk/government/organisations/uk-council-for-internet-safety

SWGfL Website: <https://swgfl.org.uk>

Online safety for professional workers helpline. Phone: 0344 381 4772*
Monday to Friday, 10am to 4pm

Welsh Government www.llyw.cymru/fframwaith-y-cyfnod-sylfaen

Online Safety Live www.saferinternet.org.uk/training-events/online-safety-live-free-online-safety-events
[Social Care Wales](http://www.diogelu.cymru/) Safeguarding Procedures ([diogelu.cymru](http://www.diogelu.cymru/))

National Cyber Security Centre, using cyber security to protect your settings:
<https://hwb.gov.wales/parthau/cadwn-ddiogel-ar-lein/canllawiau-llywodraeth-cymru/ymarferwyr-blynyddoedd-cynnar-defnyddio-seiberddiogelwch-i-ddiogelu-eich-lleoliadGu/>

Digital Communities Wales: <http://cymunedaudigidol.llyw.cymru/>

Estyn: Supplementary guidance for inspecting safeguarding in non-maintained settings [Annex 4 | Estyn \(gov.wales\)](#)

Information Commissioner's Office: 'Guidance on the use of cloud computing'
https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

Information Commissioner's Office: 'Key definitions of the Data Protection Act'
<https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/>

Safer Recruitment Consortium: Guidance for safer working practice for those working with children and young people in education settings, October 2015
<http://www.safeguardingschools.co.uk/wp-content/uploads/2015/10/Guidance-for-Safer-Working-Practices-2015-final1.pdf>

Thinkuknow: E-safety education from the National Crime Agency:
<<https://www.thinkuknow.co.uk/parents/>> &
<<https://www.thinkuknow.co.uk/Teachers/>>

Caban Y Faenol CYF