Online Safety Policy

for schools and colleges

Contents

This policy applies to all members of the Ysgol Penalltau's community (including staff, learners, volunteers, parents and carers, visitors) who have access to and are users of school's digital systems, both in and out of the school.

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/committee made up of:

- *Headteacher*
- *Online safety coordinators*
- *Staff*
- *Governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the *Governing body/governors subcommittee on:*	
The implementation of this online safety policy will be monitored by the:	*Mr. Thomas Rainsbury (Deputy DSP) and Mrs Lowri. Owen (Deputy DSP)*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body/governors subcommittee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*In the Summer Term in preparation for Governor's letter to parents.*
The online 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 online safety or incidents that have taken place. The next anticipated review date will be:	*September 2024*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*DSP and Deputy DSP, Safeguarding Governor, LA safeguarding officer, police*

The school will monitor the impact of the policy using:

- Logs of reported incidents on our Safeguarding records
- Monitoring logs of internet activity, including sites visited (supported by service provider)
- Internal monitoring data for network activity (supported by service provider)
- Surveys/questionnaires of
    - Learners
    - parents and carers
    - staff

Introduction

Ysgol Penalltau recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents/carers use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Ysgol Penalltau:

Governors:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body or governor's sub-committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor to include:

- regular meetings with the online safety co-ordinators
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs (where possible)
- reporting to relevant governors or sub-committee

Headteacher and senior leaders:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the Ysgol Penalltau's community, though the day to day responsibility for online safety may be delegated to the online safety co-ordinators
- The headteacher and another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The headteacher and senior leaders are responsible for ensuring that the online safety co-ordinators and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The headteacher or senior leaders will ensure that there is a system in place to allow for monitoring and support of those in Ysgol Penalltau who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The headteacher and senior leaders will receive regular monitoring reports from the online safety co-ordinators.

Online safety co-ordinator:

The online safety co-ordinator

- leads the online safety group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the local authority

- liaises with school technical staff
- receives reports of online safety incidents through My Concern and create a log of incidents to inform future online safety developments.
- meets regularly with online safety governor to discuss current issues, review incident logs and if possible, filtering change control logs
- attends relevant meetings with the sub-committee of governors
- reports regularly to headteacher and senior leadership team

Network manager- SRS:

The network manager- SRS is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that Ysgol Penalltau meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/internet/learning platform/Hwb/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher, senior leaders, online safety co-ordinators for investigation/action/sanction

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online 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, senior leader; online safety co-ordinators for investigation/action
- all digital communications with learners/parents and carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Learners understand and follow the online safety and acceptable use agreements
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated senior persons for Safeguarding

The designated senior persons should be trained in online 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

Online safety group

The online safety group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. At Ysgol Penallatu this group is part of the safeguarding group and other staff members and Governors with IT responsibilities. The group will also be responsible for regular reporting to the Governing Body.

Members of the online safety group will assist the online safety co-ordinators with:

- the production/review/monitoring of the school's online safety policy/documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the online safety provision

Learners:

- are responsible for using Ysgol Penalltau's digital technology systems in accordance with the learner acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Ysgol Penalltau will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website and information about national/local online safety campaigns/literature. Parents and carers will be

encouraged to support Ysgol Panteg in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website, Hwb, learning platform and online learner records
- their children's personal devices in the school

Policy Statements

Education – learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of Ysgol Penalltau's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/ /DCF) and topic areas which is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and timely intervention within classes
- Older learners in KS2 are taught to be critically aware of the materials/content they access online and are encouraged to validate the accuracy of information
- Older learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Safeguarding Persons are trained in the Prevent Duty to identify possible radicalisation and prevent/report it when necessary
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Education – parents and carers

Many parents and carers have only a limited understanding of online 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.

Ysgol Penalltau will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and the web site
- Parents and carers evenings
- High profile events/campaigns, e.g. Safer Internet Day
- Reference to the relevant web sites/publications, e.g. https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education and training – staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Ysgol Penalltau's online safety policy and acceptable use agreements.
- The online safety co-ordinators (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The online safety co-ordinators (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation, (e.g. SWGfL and HWB).
- Participation in school training/information sessions for staff, parents and Governors

Technical – infrastructure/equipment, filtering and monitoring

Ysgol Penalltau has a managed ICT service provided by an outside contractor and it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school's online safety policy/acceptable use agreements. The school should also check their local authority/other relevant body policies on these technical issues if the service is not provided by the authority.

Ysgol Penalltau will be responsible for ensuring that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Ysgol Penalltau's technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school's technical systems
- Servers, wireless systems and cabling is securely located and physical access restricted
- All users will have clearly defined access rights to the school's technical systems and devices.
- All users will be provided with a username and secure password by RSR and HWB and the school will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school' digital systems, used by the network manager (or other person) must also be available to the headteacher or other nominated senior leader and kept in a secure place.
- Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. All school provided equipment has access to secure school networks. Personal equipment may access the school's BYOD network and this is monitored. The device then has access to the wider internet which may include the school learning platform and other cloud based services such as email and data storage.

All users understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to other relevant school polices including, but not limited to, those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and

appropriate use of mobile technologies is an integral part of Ysgol Panteg's online safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners 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. Ysgol Penalltau 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 learners 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 learners in the digital/video images.
- Staff 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 will not be used for such purposes.
- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images and in accordance with the permission obtained from parents/carers.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website, class dojo and any social media platform used by the school.
- Learners' work can only be published with the permission of the learner and parents or carers.

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.

Ysgol Penalltau 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)
- Responsible persons are appointed/identified - senior information risk officer (SIRO) and information asset owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear data protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping 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" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Use school email when discussing any personal nature pertaining to the children.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Ysgol Penallatu currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults			Learners				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school/college	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time (in staff room and admin area)	X							X
Taking photos on personal mobile phones/cameras				X				X
Use of other personal mobile devices eg tablets, gaming devices				X				X
Use of personal email addresses in school/college, or on school/college network				X				X
Use of school/college email for personal emails				X				X
Use of messaging apps for school based reasons				X				X
Use of social media (school accounts)	X							X
Use of blogs				X				X

When using communication technologies Ysgol Penalltau considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

- Users must immediately report to the nominated person – in accordance with the school policy - 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 learners or parents/carers (email, chat, learning platform, etc.) must be professional in tone and content.
- Learners will be provided with individual school email addresses for educational use (accessing HWB or other Google software as instructed by the school).
- Learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social media

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

Ysgol Penalltau provides the following measures to ensure reasonable steps are in place to minimise risk of harm through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to learners, parents and 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.

When official school social media accounts are established there should be:

- A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
- Systems for reporting and dealing with abuse and misuse,
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Ysgol Penalltau's use of social media for professional purposes will be checked regularly by the online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

Ysgol Penalltau believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. Ysgol Penalltau's policy restricts usage as follows:

User Actions

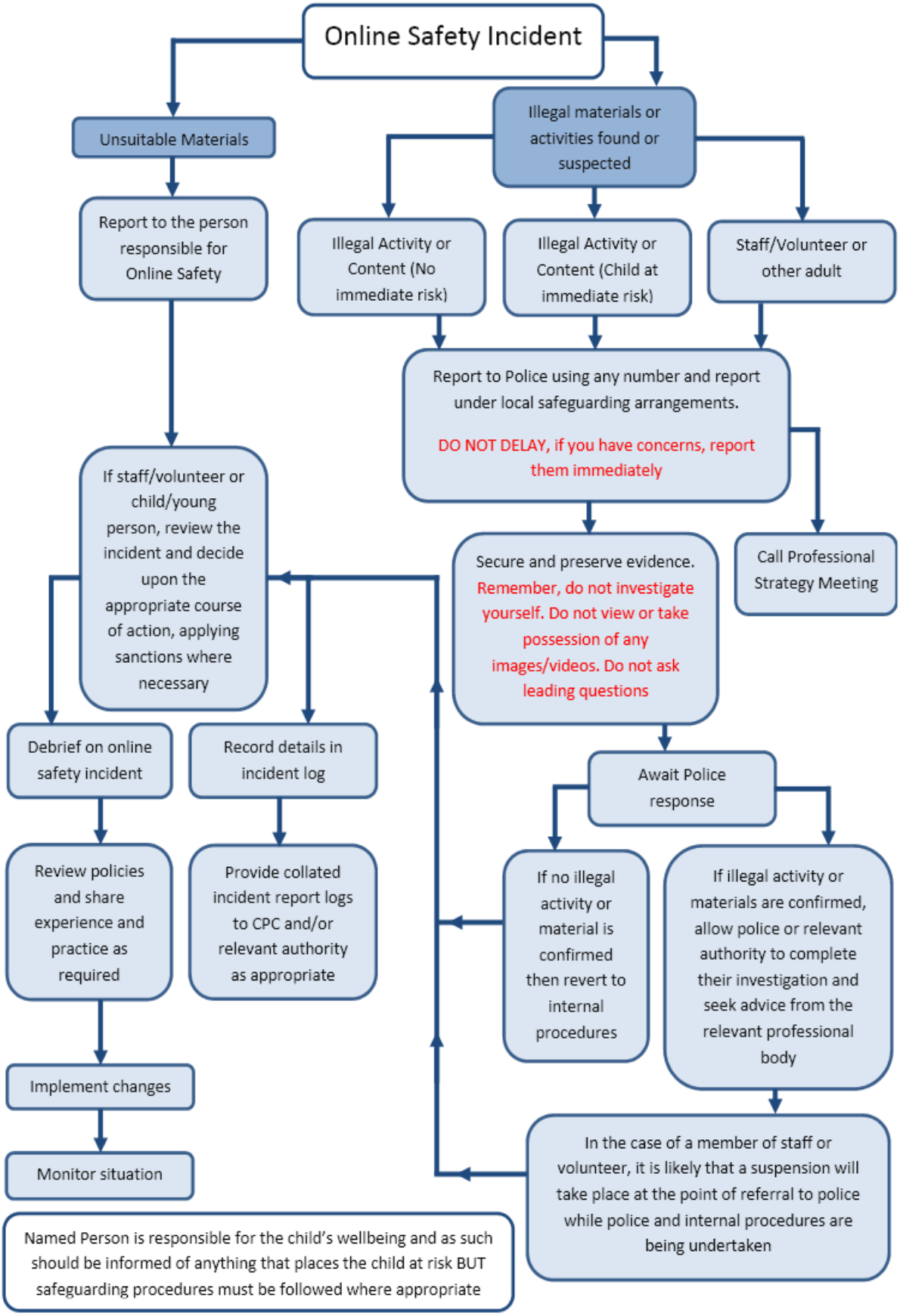
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				x	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school/college or brings the school/college into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			x			
Online gaming (non educational)					x	
Online gambling					x	
Online shopping/commerce					x	
File sharing			x			
Use of social media			x			
Use of messaging apps					x	
Use of video broadcasting, e.g. YouTube			x			

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 (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

Other Incidents

It is hoped that all members of the Ysgol Penalltau community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by local authority or national/local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents 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. It

is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Learner Actions

Incidents	Refer to class teacher/tutor	Refer to DSP or Deputy DSP	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/ security etc.	Informparents/carers	Removal of network/internet access rights	Warning	Further sanction eg. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X			
Unauthorised use of non-educational sites during lessons	X				X	X			
Unauthorised use of mobile phone/digital camera/other mobile device	X	X							
Unauthorised use of social media/messaging apps/personal email	X	X	X			X			
Unauthorised downloading or uploading of files	X								
Allowing others to access school/college network by sharing username and passwords		X	X			X			
Attempting to access or accessing the school/college network, using another learners' account	X								
Attempting to access or accessing the school/college network, using the account of a member of staff		X	X			X			
Corrupting or destroying the data of other users			X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X			
Continued infringements of the above, following previous warnings or sanctions		X	X			X	X		
Actions which could bring the school/college into disrepute or breach the integrity of the ethos of the school/college			X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X	X		

Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X	X	X	X		

Staff Actions

Incidents	Refer to DSP or Deputy DSP	Refer to Headteacher	Refer to Local Authority /HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media /personal email	x	x						
Unauthorised downloading or uploading of files	x	x			x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x						
Careless use of personal data, e.g. holding or transferring data in an insecure manner	x	x						
Deliberate actions to breach data protection or network security rules		x	x		x			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x						
Using personal email/social networking/messaging to carrying out digital communications with learners	x	x	x	x				
Actions which could compromise the staff member's professional standing		x	x					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x					

Using proxy sites or other means to subvert the school's filtering system	x				x			
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x					
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x			
Breaching copyright or licensing regulations		x	x					
Continued infringements of the above, following previous warnings or sanctions		x	x	x				

Appendix

Acknowledgements

Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school/college online safety policy templates and of the 360 degree safe Cymru online safety self review tool:

- Members of the SWGfLonline safety group
- Representatives of SW local authorities
- Representatives from a range of Welsh schools/colleges involved in consultation and pilot groups
- Plymouth University online safety

Pupil Acceptable Use Agreement Template For younger pupils

(Foundation Phase)

This is how we stay safe when we use computers:

✓ I will ask a teacher or another adult from the school if I want to use the computers

✓ I will only use activities that a teacher or another adult from the school has told or allowed me to use.

✓ I will take care of the computer and other equipment

✓ I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

✓ I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

✓ I know that if I break the rules I might not be allowed to use a computer.

Signed (child): ....(parent)

Print names: ....

Date: ..... CLASS: .....

Pupil Acceptable Use Agreement Template For older pupils

(Key Stage 2)

Pupils/parents will be made aware and asked to sign the acceptable use policy every two years (Years 3 / 4 and Year 5/ 6), or on joining the school within these years. I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

• I understand that the school will monitor my use of IT systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will be aware of "stranger danger", when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc)

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. To ensure the safety of the school's systems • I will not use memory sticks in school

• Either my parent/guardian or I will email homework to the school email address.

I have read and understand the guidelines on using school ICT systems and agree to follow them. I understand that if I do not follow these guidelines, my use of school ICT systems may be restricted.

Signed (child): ....(parent)

Print names: ....

Date: ..... CLASS: .....

Staff Acceptable Use of ICT Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This agreement and the school's e-safety and related policies are intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

ACCEPTABLE USE AGREEMENT

• I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

• I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.

• I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

• When using school ICT property outside school I will follow the same guidelines as if I were using the equipment in school.

• I will only remove school ICT property from school premises with permission of the Headteacher or a member of the Senior Leadership Team.

For my professional and personal safety:

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, tablets) out of school.

• I understand that the school ICT systems are primarily intended for educational use

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with school policies. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use chat and social networking sites for school purposes in accordance with the school's policies.

• I will only communicate with pupils and parents / carers using official school systems.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

• When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use, including seeking permission from the Headteacher or member of the Senior Leadership Team for the use of such devices.

• I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

SIGNED: .....

NAME: ..... DATE: .....