MISKIN PRIMARY SCHOOL
Ysgol Gynradd Mysgyn

Online Safety Policy

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

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

- *Headteacher/senior leaders*
- *Online safety officer/coordinator*
- *Staff – including practitioners//support staff/technical staff*
- *Governors*
- *Parents and carers*

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

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:	*online safety co-ordinator, senior leadership team*
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:	*Annually*
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:	*Summer 2018*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA, ICT manager, LA safeguarding officer, police where appropriate*

The following section outlines the online safety roles and responsibilities of individuals and groups within the school/college:

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 G*overning Body* 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-ordinator
- regular monitoring of online safety incident logs, stored in headteacher's office
- reporting to relevant governors/sub-committee/meeting

Headteacher and senior leaders: Mrs F Davies, Mrs H Davies

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school, though the day to day responsibility for online safety may be delegated to the online safety co-ordinator
- 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/senior leaders are responsible for ensuring that the online safety co-ordinator 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/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school 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/senior leaders will receive regular feedback from the online safety co-ordinator.

Online safety co-ordinator: Mrs F Davies, Mrs H Davies

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 online safety policies/documents
- 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 technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to online safety governor to discuss current issues and review incident logs

Network manager/technical staff: ExtraScope

The network manager/technical staff is responsible for ensuring:

- that the *school* technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the required online safety technical requirements as identified by the local authority 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 for investigation.
- that monitoring software/systems are implemented and updated as agreed in school policies
- that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

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 h*eadteacher* for investigation/ action
- all digital communications with learners/parents and carers should be on a professional level
- 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 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

Designated senior person

The designated senior person 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. 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-ordinator, as with:

- the production/review/monitoring of the school 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
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

Learners:

- are responsible for using the school 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, if related to their membership of the 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. The school will take every opportunity to help parents understand these issues through *letters, website, Hwb, and information about national/local online safety campaigns*. Parents and carers will be encouraged to support the school 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 the website and Hwb

Education – learners

The education of learners in online safety is an essential part of the school'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 should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be 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 and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and classroom activities
- Learners should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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 may 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.

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

Curriculum activities

- *Letters, web site, Hwb*
- *Parents and carers evenings/sessions*
- *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/volunteers

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:

- 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 the school online safety policy and acceptable use agreements.
- The online safety co-ordinator 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/team meetings/INSET days.
- The online safety co-ordinator 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).
- Participation in school/college training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school/college technical systems and devices.
- For PurpleMash, all users will be provided with a username and secure password by the *online safety co-ordinator who will keep an up to date record of users and their usernames*. Users are responsible for the security of their username and password *and will be required to change their password every year.* (The school may choose to use group or class log-ons and passwords for nursery, but need to be aware of the associated risks)
- Extrascope 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. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school/college site unless safely encrypted or otherwise secured.

Mobile technologies

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

	School/college Devices				
	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned
Allowed in school	Yes	Yes	yes	No	Yes
Full network access	No	No	No	No	No
Internet only	No	No	No	No	Yes
No network access	No	No	No	Yes	Yes

Use of digital and video images

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/ college 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 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
- 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
- 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.

Data Protection

The school must ensure that:

- It adheres to LA Data Protection requirements

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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected

- the data must be securely deleted from the device, in line with school/college policy once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school/college 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.
- Whole class/group email addresses may be used for educational use.
- 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.

Social media

All staff are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to 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 personal 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
- 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

Responding to incidents of misuse

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 for responding to online safety incidents and report immediately to the police.

Report to parents

Report to parents

Other Incidents

It is hoped that all members of the school will be responsible users of digital technologies, who understand and follow school/college 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	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/ security etc.	Inform parents/ carers	Removal of network/ internet access rights	Warning	Further sanction eg. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X							

Unauthorised use of mobile phone/digital camera/other mobile device		X						
Unauthorised use of social media/ messaging apps/ personal email		X						
Unauthorised downloading or uploading of files				X				
Allowing others to access school/college network by sharing username and passwords		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						
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	X	X

Continued infringements of the above, following previous warnings or sanctions					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	
Using proxy sites or other means to subvert the school/college's filtering system				X				
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
Deliberately accessing or trying to access offensive or pornographic material		X		X	X		X	X
21 21	X	X						

Staff Actions

Incidents	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	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		
Allowing others to access school/college network by sharing username and passwords or attempting to access or accessing the school/college network, using another person's account	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	X			X		

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		
Using personal email/ social networking/ messaging to carrying out digital communications with learners	X				X		
Actions which could compromise the staff member's professional standing	X				X		
Actions which could bring the school/ college 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/ college's filtering system				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
Breaching copyright or licensing regulations		X					X
Continued infringements of the above, following previous warnings or sanctions							X

Date endorsed by Governing Body _________________________

Policy to be reviewed _______________________________