



Online Safety Policy

June 2020

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Schedule for development/monitoring/review

This online safety policy was approved by the <i>governing</i> body on:	
The implementation of this online safety policy will be monitored by the:	
Monitoring will take place at regular intervals:	
The <i>governing body</i> 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:	
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:	
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA ICT manager, LA safeguarding officer, police</i>

The school will monitor the impact of the policy using:

- Reports of reported incidents on 'My Concern'
- Professional dialogue with all staff via INSET, staff meetings and professional learning sessions.
- Assessment and coverage of DCF online safety skills by teachers on Building Blocks.
- Surveys/questionnaires of:
 - learners
 - parents and carers
 - staff.

Roles and responsibility

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

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* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body takes on the role of online safety governor to include:

- meetings with the online safety lead/online safety group members
- monitoring of online safety incident reports on My Concern at Governors' meeting

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety may be delegated to the online safety lead.
- The headteacher and (at least) 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 lead 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 monitoring reports from the online safety lead/online safety group SLT members.

Online safety lead.

The online safety lead:

- 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 school technical staff
- receives reports of online safety incidents and uses this information to inform future online safety developments
- meets with online safety governor to discuss current issues, review online safety My Concern reports
- reports to headteacher/senior leadership team with online safety issues/concerns.

Technical staff

Technical staff and the Vale of Glamorgan's LEA are responsible for ensuring that:

- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school 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
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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
- the use of the Hwb access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher, SLT; online safety lead for investigation/action/sanction

Teaching and support staff

These individuals 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 lead* for investigation/action.
- All concerns are recorded on 'My Concern'.
- 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 and codes of conducts displayed in their classrooms
- KS2 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, i.e. these are reported to the LEA and the sites will then be blocked.

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
- online bullying.

Online safety group

The online safety group provides a consultative group that has wide representation from the school and parents 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 senior leaders and the governing body.

Members of the online safety group will assist the online safety lead with:

- the production/review/monitoring of the school online safety policy/documents
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident concerns where possible
- consulting stakeholders where possible– 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.

An online safety group terms of reference template can be found in the appendices.

Learners

These individuals:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and respective codes of conducts displayed in classrooms
- KS2 pupils should 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.
- 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 and carers understand these issues through parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature. 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 parents'/carers' sections of the website, Hwb, learning platform and online learner records
- their children's personal devices in the school (where this is allowed).

Policy statements:

Education – learners

While 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 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 in order to become responsible digital citizens.

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 tutorial/pastoral activities.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- 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.
- 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.

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

- letters, newsletters, web site, learning platform, Hwb
- parents and carers evenings/sessions
- high profile events/campaigns, e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. hwb.wales.gov.uk/
www.saferinternet.org.uk/ www.childnet.com/parents-and-carers

Education – the wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies, digital literacy and online safety
- online safety messages targeted towards grandparents and other relatives as well as parents via newsletters, Hwb and the school's website.
- the school learning platform, Hwb, website will provide online safety information for the wider community

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:

- 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 through forms surveys.
- 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 lead and/or DCF lead 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 lead and/or DCF lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions. All governors have to undertake safeguarding training. The training is in line with the revised “Keeping Learners Safe” guidance that was issued by Welsh Government which highlight online safety as a key area.

Technical – infrastructure/equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements <https://hwb.gov.wales/support-centre/education-digital-standards/> and <https://hwb.gov.wales/support-centre/education-digital-guidance-for-schools/>
- 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 school networks and system will be protected by secure passwords.
- The master account passwords for the school systems are kept in a secure place.
- All users have clearly defined access rights to school technical systems and devices.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by Mr Mike Chapman and Miss Kelly Bladon who will keep an up to date record of users and their usernames.
- Passwords should be long and strong. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity in foundation phase should be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- All individual pupil passwords should be stored in personal individual books/folders.
- Internet access is filtered for all users.

- There is a clear process in place to deal with requests for filtering changes i.e. access to inappropriate sites are reported to the LEA to block.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed. Pupils, staff and parents will report online safety incidents to the Safeguarding officer and concerns will be reported and recorded on 'My Concern'.

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/college's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies 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 should be an integral part of the school's online safety education programme.

	School devices			Personal 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	Yes	Yes	Yes	No	Yes
Internet only	Yes	Yes	Yes	No	Yes
No network access	Yes	Yes	Yes	No	Yes

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 online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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, e.g. 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 is 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. Those images should only be taken on school equipment; the personal equipment of staff should 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.
- 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 or social media sites
- 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 current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy. (see separate Data Protection Policy)
- it implements the data protection principles and is able to demonstrate that it does so.
- it has paid the appropriate fee Information Commissioner's Office (ICO)
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. (Tim Cousins, Vale of Glamorgan Council DPO, Mike Chapman School based Data Lead)
- it has an 'information asset register' (GDPRis) in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it
- the information asset register (GDPRis) lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- 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. The school should develop and implement a 'retention schedule' to support this (information on Hwb for all staff access)
- data held must be accurate and up to date where this is necessary for the purpose you hold it for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school / college looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them

- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- it has undertaken appropriate due diligence and has GDPR compliant contracts in place with any data processors
- it understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools and colleges should consider using the [Wales Accord on Sharing Personal Information](#) toolkit to support regular data sharing between data controllers
- there are clear and understood policies and routines for the deletion and disposal of data (SRS school retention schedule)
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents. (GDPRis)
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- device must be password protected.
data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- device must be protected by up to date virus and malware checking software

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- will not transfer any school personal data to personal devices except as in line with school policy
- 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.

Communication technologies

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

	Staff and 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	X							X
Use of mobile phones in lessons	X							X
Use of mobile phones in social time	X							X
Taking photos on mobile phones/cameras	X							X
Use of other mobile devices, e.g. tablets, gaming devices	X							X
Use of personal e-mail addresses in school, or on school network		X						X
Use of school e-mail for personal e-mails								X
Use of messaging apps	X							X
Use of social media	X							X
Use of blogs	X							X

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

- the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and learners should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- 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 (e-mail, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications
- all learners will be provided with individual school e-mail addresses 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.

- personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff,

Social media

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools/colleges and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools/colleges and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- training being provided including acceptable use, social media risks, checking of settings, data protection and 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
- 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.
- *The school permits reasonable and appropriate access to private social media sites.*

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.

School use of social media for professional purposes will be checked regularly by a senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

Some internet activity such as accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities such as online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school 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. The school 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 or brings the school 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				

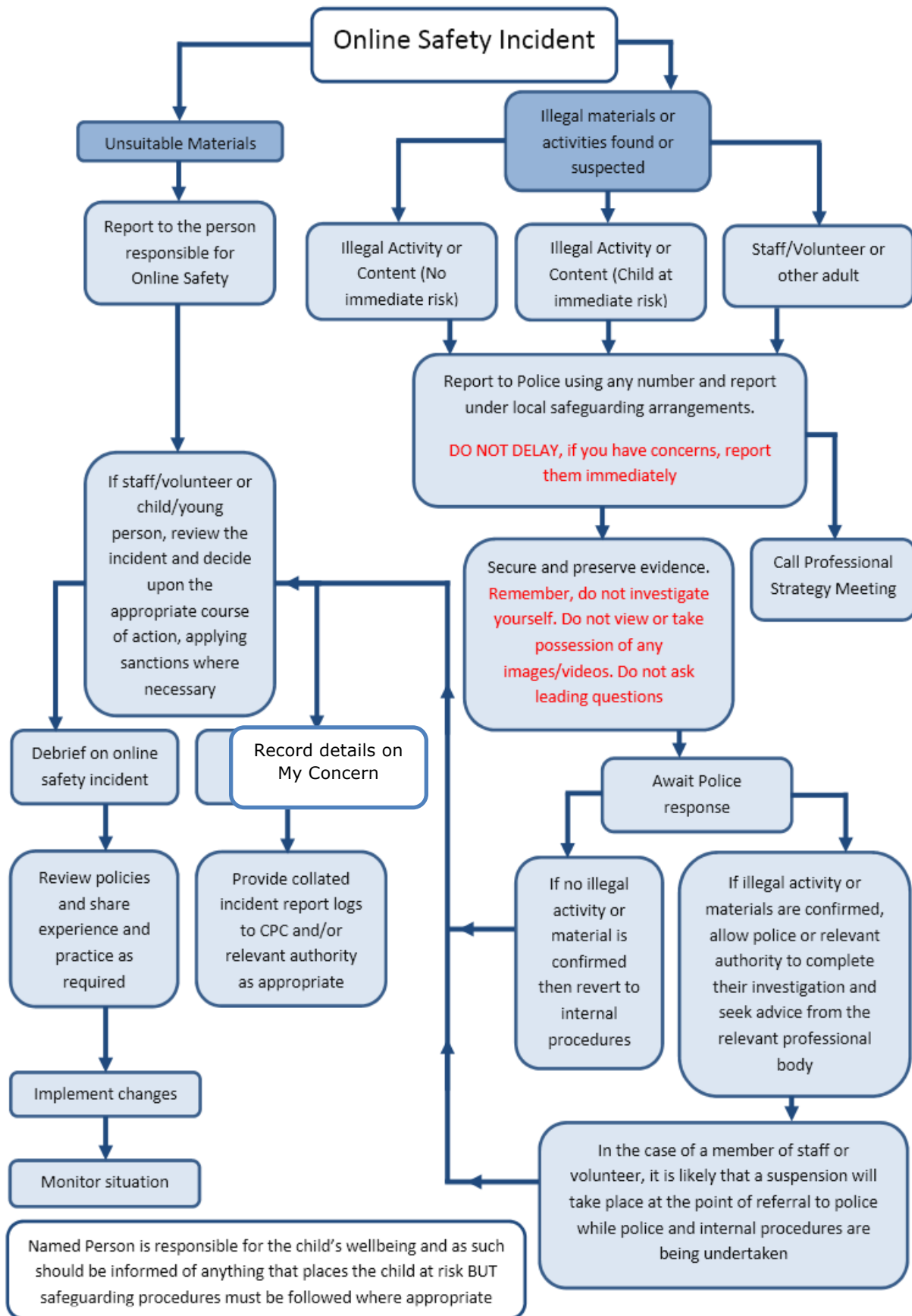
Responding to incidents of misuse

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 website (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 and appendix) for responding to online safety incidents and report immediately to the police.

All staff have been issued with a flowchart to help them know how to report incidents of misuse



Other incidents

It is hoped that all members of the school 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/volunteer 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 Headteacher/Principal	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, e.g. 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					
Unauthorised use of non-educational sites during lessons.	X	X		X	X	X	X	
Unauthorised use of mobile phone/digital camera/other mobile device.	X	X		X	X	X	X	
Unauthorised use of social media/messaging apps/personal e-mail.	X	X		X	X	X	X	
Unauthorised downloading or uploading of files.	X	X		X	X	X	X	
Allowing others to access school network by sharing username and passwords.	X	X		X	X	X	X	
Attempting to access or accessing the school network, using another learners' account.	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff.	X	X		X	X	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					
Continued infringements of the above, following previous warnings or sanctions.		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					
Deliberately accessing or trying to access offensive or pornographic material.		X	X					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X					

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/HR	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 e-mail		X	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			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X			X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		X	X				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				X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.		X	X				X	X
Using proxy sites or other means to subvert the school's/college's filtering system.		X	X	X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X	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				X	
Continued infringements of the above, following previous warnings or sanctions.		X	X	X			X	X

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 online safety policy templates and of the 360 degree safe Cymru online safety self review tool:

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

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2018. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2018