Online Safety Policy

YSGOL GATHOLIG SANTES FAIR

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).

Online Safety Policy

Date	Review Date	Coordinator	Nominated Governor
2.9.2019	**July 2020**	**Chelsea Ford**	**Gareth Hughes**

At St Mary’s Catholic School, we place Christ at the centre of all that we are and all that we do. We aim to promote the fullness of Christian life through an education in which faith, culture and life are brought into harmony, creating a community based on the Gospel values of love, care and respect.

This harmony within our Catholic school community forms the basis on which our children will develop Christian values and motivation that will enable them to act and make choices in life.

In our multi-faith society, confident in our personal position in religious matters, we work to promote respect for the rights and dignity of others.

The governors, head teacher, staff, parents and pupils will seek and develop ever new ways of placing the person of Christ and the teachings of the Catholic Church at the centre of school life whilst at the same time engaging positively with changes and developments in education, in this way the school contributes to the common good of the area and its culture.

Our priority is to create an environment where every child travels a journey of faith, grows in self-esteem and can truly ***, ‘Live, Learn and Grow in Christ’s Love.’***

Contents

Development/monitoring/review of this policy

This online safety policy has been developed by Chelsea Ford (ICT Coordinator), Richard Jones (Headteacher), Brioni Somers (Teacher), Gareth Hughes (Govenor) and the school's Digital Heroes group

This online safety policy was approved by the *governing body/governors sub-committee on:*	
The implementation of this online safety policy will be monitored by the:	Chelsea Ford (ICT Coordinator) Richard Jones (Headteacher) Gareth Hughes (Governor) Digital Heroes Group
Monitoring will take place at regular intervals:	Twice a year January and July
The *governing body/governors sub-committee* 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:	Twice a year January and July
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:	Twice a year January and July
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA safeguarding officer* *Added to My Concern database*

The school will monitor the impact of the policy using:

- Logs of reported incidents (book to be kept in the safe in school office)
- Any serious incidents will be logged on My Concern (Safeguarding Programme)
- Surveys/questionnaires of
  - Learners
  - parents and carers
  - staff

Roles and responsibilities

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 G*overning Body/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[1] to include:

- regular meetings with the online safety coordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs and monitoring of filtering logs (where possible)
- reporting to relevant governors/sub-committee/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 coordinator/officer
- 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 coordinator/officer 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 coordinator/officer

The online safety co-ordinator (Miss Chelsea Ford)

- 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/relevant body
- liaises with (school/) technical staff
- receives reports of online safety incidents and creates 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 meeting/sub-committee of governors
- reports regularly to headteacher/senior leadership team

Network manager/technical staff

The network manager/technical staff (CYNNAL) is responsible for ensuring:

- 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 network/internet/learning platform/Hwb/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Group for investigation/action/sanction
- (if present) monitoring software/systems are implemented and updated as agreed in school policies
- 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

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 user agreement (AUA)
- they report any suspected misuse or problem to the Online Safety Group
- 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 person (Richard Jones)

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 community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. 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 coordinator/officer with:

- the production/review/monitoring of the school online safety policy/documents
- the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- mapping and reviewing the online safety education 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.

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
- 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 and digital cameras. They should also know and understand policies on the taking/use of images and on online 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 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).

Community users

Community users who access school systems/website/Hwb/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Policy statements

Education – learners

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/DCF) and topic areas and should be regularly revisited (Cornerstones DCF Expanded Task and Safety Sessions)
- 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. (Counter Terrorism and Securities Act 2015)
- 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:

- Curriculum activities
- 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.* https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers placed as links on the school website and communication guides.

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.
- The school/ learning platform, Hwb, website will provide online safety information for the wider community
- Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (done through Digital Communities Wales Training Events)

Education and training – staff/volunteers

- Formal online safety training will be made available to staff through the year. 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 the school online safety policy and acceptable use agreements.
- The online safety coordinator/officer will receive regular updates through attendance at external training events, 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 coordinator 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/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

- attendance at training provided by the local authority/National Governors Association/or other relevant organisation,
- participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

Cynnal 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 will also need 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
- 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.
- Good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine, including the keeping of copies off-site.
- All school networks and system will be protected by secure passwords
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Cynnal and will be reviewed, at least annually, by the online safety group
- 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 secure password by the coordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. These can be changed via Hwb. The ‘Hwb Digital Champion’ for the school is – Chelsea Ford.
- Records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be be securely kept when not required by the user.

- Cynnal (computer system software) and Richard Jones are both responsible for ensuring that software licence logs (INCERTS, Cornerstones, My Concern, ZuluDesk) 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
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet (Counter Terrorism and Securities Act 2015)
- 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.
- An agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreement is in place regarding the extent of personal use that users (staff) and their family members are allowed on school devices that may be used out of school. The staff each have an iPad that they are allowed to take home. Family members are not to use them.

Staff can use their own personal removable media (e.g. memory sticks/CDs/DVDs) on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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/school'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 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 should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school allows:

	School Devices		Personal Devices	
	School owned for child use	School owned for staff use	Student owned	Staff owned
Allowed in school/	yes	yes	No*	Yes
Full network access	no	yes	No	no
Internet only	yes	yes	No	Yes

*on residential trip, Year 6 children are allowed to bring them

Personal devices

- Staff/visitors are allowed mobile devices for personal use
- They must be kept secured in a bag or locker away from children when not in use
- Staff/visitors can login and use the school wifi

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, eg., on social networking sites.
- 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
- 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. See Website Policy for more details.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website. A copy of whole school allowed consent will be given to all teaching staff.
- Learners' work can only be published with the permission of the learner and parents or carers. See separate policy for SeeSaw Application.

Data protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy
- Implements the data protection principles and is able to demonstrate that it does so.
- 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.
- has an 'information asset register' 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 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
- 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 / school looks after their data and what their rights are in a clear Privacy Notice
- 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 schools 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
- 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.
- 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:

- It is advised that a USB removal device must be password protected
- 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 understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- 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

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							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, Hwb, may be regarded as safe and secure and is monitored through a filtering system (e.g. flagged up words). Users should be aware that e-mail communications are monitored through a filtering system (e.g. flagged up words).
- 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. See Social Media Policy for advice on using social media.
- whole class/group e-mail addresses may be used at Foundation Stage , while learners at Key Stage 2 and above will be provided with individual school e-mail addresses for educational use (Hwb Mail accounts)

- 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 about staff (except qualification details) or photos 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 and local authorities have a duty of care to provide a safe learning environment for learners 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, 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 should be strict and private and are regularly checked to minimise risk of loss of personal information.

When official school social media accounts (Facebook and Twitter) are used there is a separate policy for;

- who is allowed to post to the site and 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.

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 (See school Social Media Policy)

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	

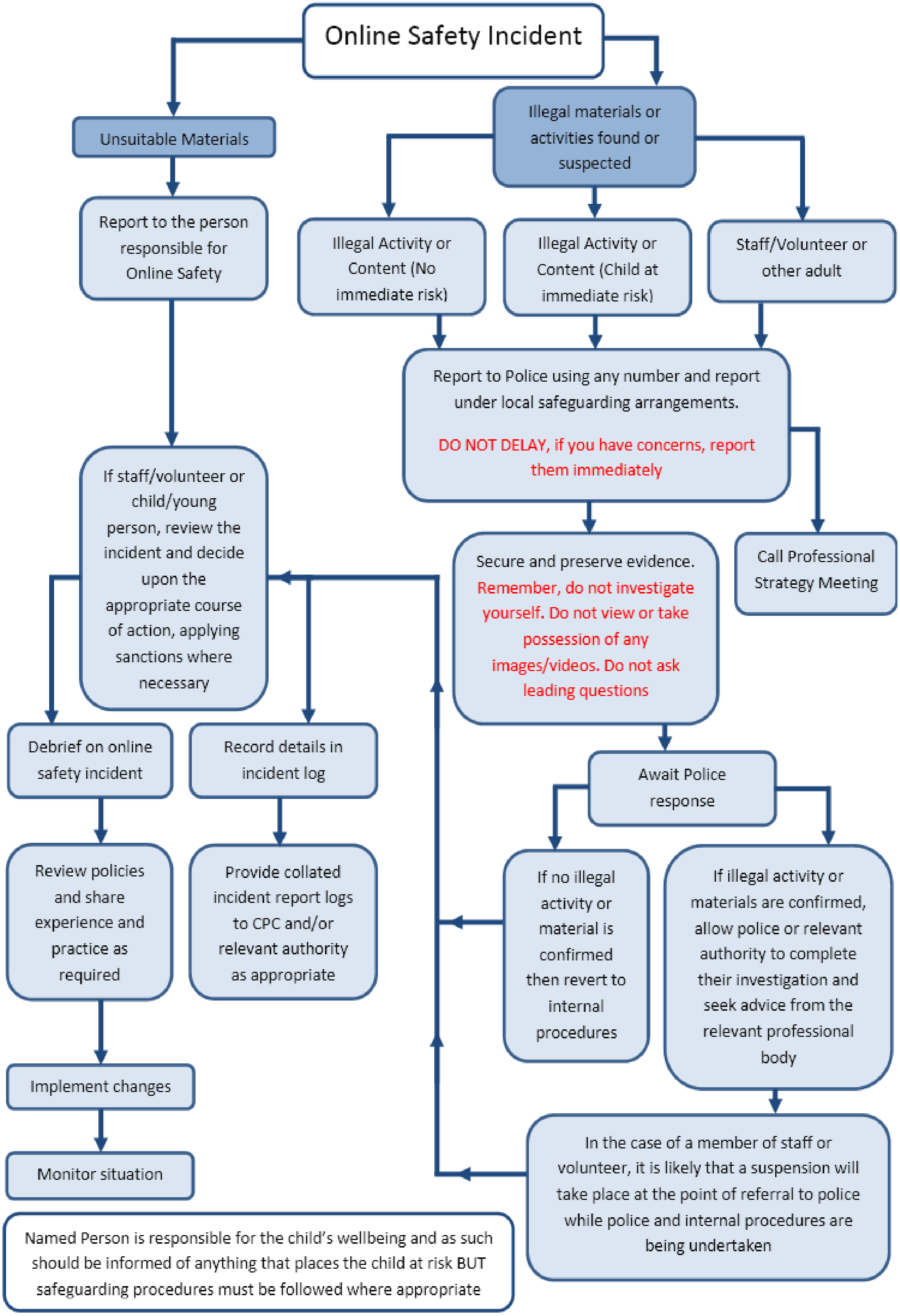
Online gaming (educational)		X			
Online gaming (non educational)				X	
Online gambling				X	
Online shopping/commerce			X		
File sharing	X				
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting, e.g. YouTube	X				

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



Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to CPC and/or relevant authority as appropriate

Illegal materials or activities found or suspected

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

Call Professional Strategy Meeting

Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions

Await Police response

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

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 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.

- Report can be made to any member of the Online Safety Group (except the Digital Heroes).
- Conduct the procedure using a designated computer (in the main office) 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 DSP	Refer to Headteacher	Refer to Police	Refer to Cynnal 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	X					
Unauthorised use of non-educational sites during lessons.	X							X	
Unauthorised use of mobile phone/digital camera/other mobile device.	X							X	
Unauthorised use of social media/messaging apps/personal e-mail.	X							X	
Unauthorised downloading or uploading of files.	X							X	
Allowing others to access school network by sharing username and passwords.	X							X	
Attempting to access or accessing the school network, using another learners' account.			X			X			X
Attempting to access or accessing the school network, using the account of a member of staff.			X			X			
Corrupting or destroying the data of other users.	X		X		X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.			X		X	X			X
Continued infringements of the above, following previous warnings or sanctions.			X	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		
Using proxy sites or other means to subvert the school'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			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X		X		X				

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to Cynnal 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
Inappropriate personal use of the internet/social media/personal e-mail		X				X		
Unauthorised downloading or uploading of files.		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		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		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		
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/school's filtering system.		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
Breaching copyright or licensing regulations.		X	X	X		X		
Continued infringements of the above, following previous warnings or sanctions.			X	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 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/schools involved in consultation and pilot groups
- Plymouth University online safety

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.

Appendices – Section A - Acceptable Use Agreement

A1 Learner Acceptable Use agreement template (younger children)

- A2 Learner Acceptable Use agreement template (older children)
- A3 Staff and Volunteers Acceptable Use Agreement template
- A4 Parents /Carers Acceptable Use Agreement template
- A5 Community Users Acceptable Use Agreement template

Appendices – Section B – Specific Policies

- B1 Technical security policy template
- B2 Personal data advice and guidance

- B3 Mobile technologies policy template
- B4 Social media policy template

- B5 Online safety group terms of reference

Appendices – Section C – Supporting documents and links

- C1 Responding to incidents of misuse – flowchart
- C2 Record of reviewing sites (for internet misuse)

- C3 Reporting log template

- C4 Training needs audit template

- C5 Summary of legislation

- C6 Links to other organisations and documents

- C7 Glossary of terms

A1 Learner Acceptable Use Agreement (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/tablet.

Child Name: ....

Signed (parent): ....

Date (parent): ....

Learner Acceptable Use Agreement (Key Stage Two)

School policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools/schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safer internet access at all times.

This Acceptable use agreement is intended to ensure:

- that learners will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Acceptable use agreement

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

For my own personal safety:

- I understand that the school will monitor my use of 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 online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the school systems or devices for online gaming, file sharing, or video broadcasting (eg YouTube), if I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others’ work and property and will only access, copy, remove or alter any other user’s files, with the owner’s knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will only take or distribute images of others with their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal device(s) in school if I have permission I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a school device, if I have permission

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- where work is protected by copyright, I will not try to download copies (including music and videos)
- when I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information)
- I understand that if I fail to comply with this acceptable use agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below / on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Name of Learner:...

Group/Class ....

Signed: ....

Date: ....

Parent/Carer Countersignature ....

Staff (and volunteer) acceptable use agreement

School policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/schools and in their lives outside school. The internet and other digital 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 safer internet access at all times.

This acceptable use agreement is 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 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 digital technologies in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technologies to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use agreement

I understand that I must use school digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

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 (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- 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 only access, copy, remove or alter any other user's files, with their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's/school's policy on the use of digital/video images. I will only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the school website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use social networking sites in school in accordance with the school's policies.

- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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 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. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/LA Personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened (Using Yellow Log Book in School Office)

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology 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.

Staff/Volunteer Name: ---

Signed: .... Date ....

Parent/carer acceptable use agreement

Digital technologies have become integral to the lives of children and young people, both within schools/schools and outside school. These technologies provide powerful tools, which create new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's/school's work.

Permission Form

Parent/Carers Name:.. Learner's Name ....

Learner's Name ....

Date:..

As the parent/carer of the above learner(s), I give permission for my son/daughter to have access to the internet and to digital technology systems at school.

Either: (KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (Foundation)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital technology systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the digital technology systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

The Senior Management Team and Office Personnel only will have access to this form.

It will be stored securely in the main School Office

It will be stored for the duration your child (children) will attend the school

It will then be destroyed by paper shredder

Signed .... Date: ....

DIGITAL IMAGES

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form will be electronic	The images
The Senior Management Team and Office Personnel only will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
Stored securely on the computer	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

School personal data advice and guidance- for use alongside the Data Protection Policy

School personal data handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools/schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any-personal data breach
- the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
- it is a legal requirement for all schools / schools to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools / Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools / Schools will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

Introduction

Schools / Schools and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data, that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority / Parent Organisation).

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represents a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaces the Data Protection Act 1998. These two documents are intended to be read side-by-side.

The GDPR provides the principles and rights which apply across the European Union. The Data Protection Act 2018 covers the areas outside of the EU GDPR and provides the UK-specific details such as; how to handle education and safeguarding information.

Are schools / schools in Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools / schools and the personal data required in a variety of forms to operate a school this means that all educational establishments in the UK are required to comply.

Guidance for schools / schools is available on the Information Commissioner's Office website including information about the new regulations.

Personal Data

The school / school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information that relates to an identified or identifiable living individual This will include:

- personal information about members of the school community – including learners, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- curricular / academic data e.g. class lists, learner progress records, reports, references
- professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Special categories of personal data

The following is a list of personal data listed in the GDPR as a 'special category'.

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Consent

Consent (which is one of the lawful bases to use data) under the regulation has changed. Consent is defined as:

"in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools / schools should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds) , so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.
- if your school or school requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Consent is just one of the six lawful bases for processing data:

1. Consent
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
3. Legal obligation: the processing is necessary for you to comply with the law
4. Vital interests: the processing is necessary to protect someone's life
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks).

Previously maintained schools / schools were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools /schools). However, public bodies should consider using the Public Task lawful base whenever they are undertaking a task that is part of their statutory function.

Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what are the risks to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

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

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

In the GDPR, organisations are required to keep records of processing activity. This must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the data

Data Breaches

From 25 May 2018, if you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The school/ school should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

Data Mapping

The process of data mapping is designed to help schools / schools identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your learners then this processor has obligations on behalf of the school to ensure that processing takes place in compliance with data protection laws.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – Unlikely to be used in a school context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and schools, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the individual. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

Individuals have the right to know:

- if the Controller holds personal data about them
- a description of that data

- the purpose for which the data is processed
- the sources of that data
- to whom the data may be disclosed
- a copy of all the personal data that is held about them.

A school must not disclose

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school or school must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Fee

The school should pay the relevant fee to the Information Commissioner's Office (ICO).

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data

- monitor compliance by the controller with data protection laws

The school may also wish to appoint a Data Manager. Schools/schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / school's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools / schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school to consider whether the requested information should be released into the public domain. FOI links to data protection law whenever a request includes personal data. Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/school's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests

- ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's / school's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / schools complete the Guide to Information for Schools.

Information to Parents/carers – the Privacy Notice

In order to comply with the fair processing requirements in data protection law, the school will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

Parental permission for use of cloud hosted services

Schools / schools that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools / schools that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools / schools under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act
- They must provide alternative means for accessing services where a parent or pupil has refused consent

New advice to schools / schools makes it clear that they are not able to use pupils' biometric data without parental consent. Schools / schools may wish to incorporate the parental permission procedures into revised consent processes. (see Appendix A4 Parent / Carer Acceptable Use Agreement)

Privacy and Electronic Communications

Schools / schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

School policy Online safety group terms of reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the full governing body.

2. MEMBERSHIP

2.1 The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (n.b. in small schools/schools one member of staff may hold more than one of these posts): [add/delete where appropriate]

- Senior Leadership Team (SLT) member/s
- safeguarding officer
- teaching staff member
- support staff member
- online safety co-ordinator (not ICT coordinator by default)
- governor
- parent/carer
- technical support staff (where possible)
- community users (where appropriate)
- *learner representation* – for advice and feedback. *Learner voice is essential in the make up of the online safety group, but learners would only be expected to take part in meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the group to provide advice and assistance where necessary

2.3 Group members must declare a conflict of interest if any incidents being discussed directly involve

themselves or members of their families.

2.4 Group members must be aware that many issues discussed by this group could be of a sensitive or

confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave

the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The group should select a suitable chairperson from within the group. Their responsibilities include:

- scheduling meetings and notifying group members
- inviting other people to attend meetings when required by the group
- guiding the meeting according to the agenda and time available
- ensuring all discussion items end with a decision, action or definite outcome
- making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the online safety co-ordinator (or other relevant person) with the following: [add/delete where relevant]

- to keep up to date with new developments in the area of online safety
- to (at least) annually review and develop the online safety policy in line with new technologies and incidents
- to monitor the delivery and impact of the online safety policy
- to monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- to co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:
    - staff meetings
    - learner forums (for advice and feedback)
    - governors meetings
    - surveys/questionnaires for learners, parents/carers and staff
    - parents evenings
    - website/learning platform/newsletters
    - online safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - other methods
- to ensure that monitoring is carried out of Internet sites used across the school (if possible)
- to monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- to monitor the safe use of data across the [school]
- to monitor incidents involving online bullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all group members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT): ---

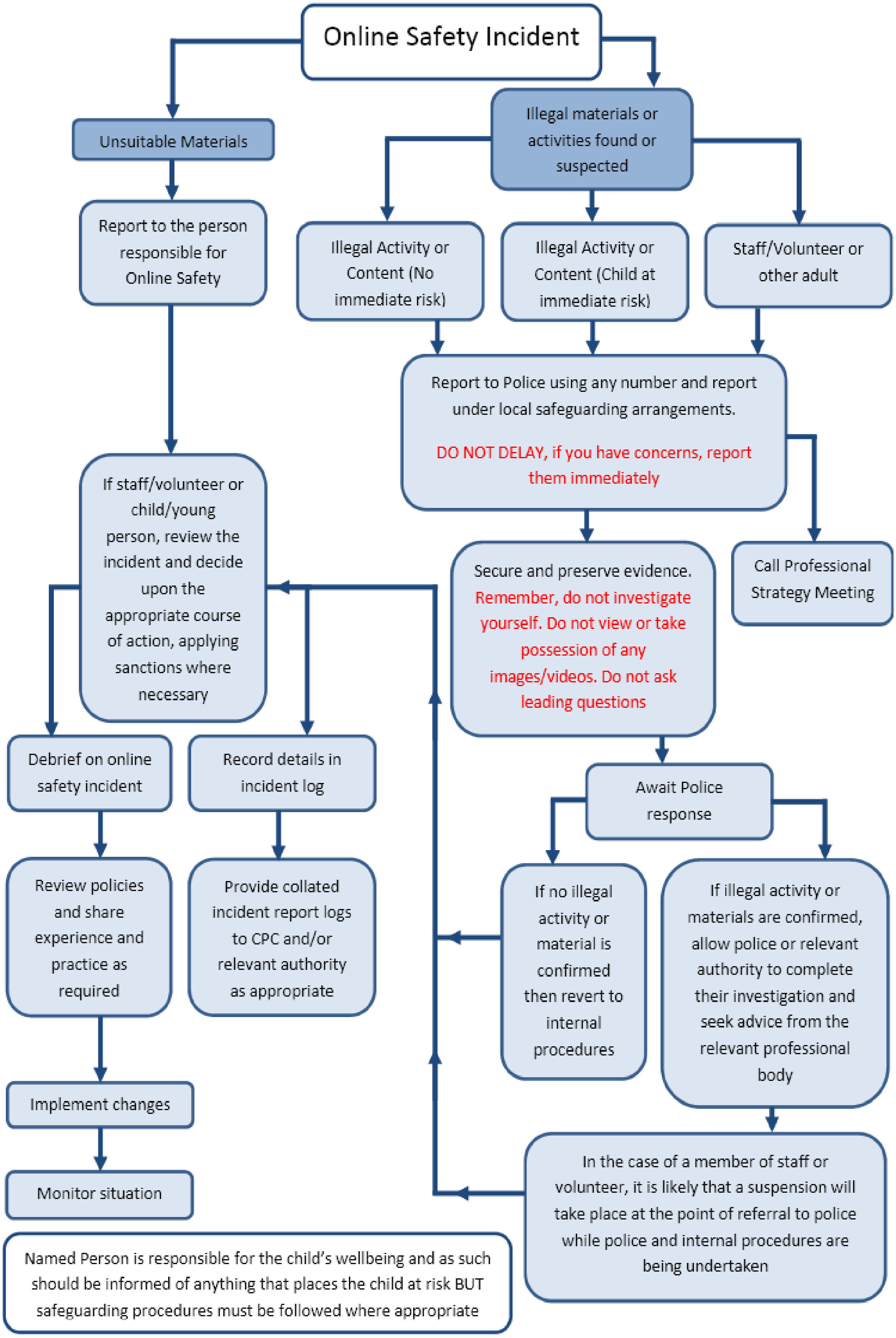
Date: ---

Date for review: ---

Acknowledgement

This template terms of reference document is based on one provided to schools/schools by Somerset County Council

C1 Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to CPC and/or relevant authority as appropriate

Illegal materials or activities found or suspected

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

Call Professional Strategy Meeting

Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions

Await Police response

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

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

C2 Record of reviewing devices/internet sites

(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

C3 Reporting Log Template

Group: ....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

C4 Training Needs Audit Log Template

Group: ....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date		

Summary of Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority;
- obtain unauthorised access to a computer;
- “eavesdrop” on a computer;
- make unauthorised use of computer time or facilities;
- maliciously corrupt or erase data or programs;
- deny access to authorised users.

Data Protection Act 2018

Controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data

- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- establish the facts
- ascertain compliance with regulatory or self-regulatory practices or procedures
- demonstrate standards, which are or ought to be achieved by persons using the system
- investigate or detect unauthorised use of the communications system
- prevent or detect crime or in the interests of national security
- ensure the effective operation of the system
- monitoring but not recording is also permissible in order to
- ascertain whether the communication is business or personal
- protect or support help line staff

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. You Tube).

Criminal Justice & Public Order Act 1994/Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006/Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly

- prohibition of discrimination
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

The Protection of Freedoms Act 2012

Requires schools/schools to seek permission from a parent/carer to use Biometric systems

The Counter-Terrorism and Security Act 2015

Places a responsibility on schools to participate in work to prevent people from being drawn into terrorism, and challenge extremist ideas that support or are shared by terrorist groups.