Ysgol Gynradd Gymraeg Hamadryad

Online Safety Policy

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 devices on the school site (where allowed).

Date created: [9/12/25]

Next review date: [9/12/26]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of [*INSERT SCHOOL NAME*] to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety 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 devices on the school site (where allowed).

[*INSERT SCHOOL NAME*] will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *[insert group/committee name e.g. Online Safety Group]* made up of: (delete/add as appropriate)

- *headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/education practitioners/support staff/technical staff*
- *governors*
- *parents and carers*
- *community users*

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

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*Insert date*
The implementation of this Online Safety Policy will be monitored by:	*Insert name of individual/group/committee (e.g. online safety lead, senior leadership team, other relevant group)*
Monitoring will take place at regular intervals:	*Every year*
The *governing body* 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:	*Every year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*9.12.26*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Insert names/titles of relevant persons/agencies, e.g. LA ICT co-ordinator, head teacher, LA safeguarding officer, police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to an appropriate member of the senior leadership team.
- 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[2].
- The headteacher/senior leaders are responsible for ensuring that all staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and 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.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

Keeping Learners Safe states:

[1] In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

[2] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority HR/other relevant body disciplinary procedures.

2.38. "All governors, including the chair of governors, should be given access to safeguarding and child protection training to ensure a basic and consistent level of awareness. This training includes, but is not limited to, the Keeping learners safe modules. Governing bodies are responsible for ensuring the education setting policies and procedures for safeguarding meet statutory requirements, and all governors should know what to do if they have concerns about a child."

3.61. "The DSP should liaise with the designated governor for safeguarding so that the designated governor can report on safeguarding issues, irrespective of whether the issue is online or offline, to the governing body. Reports to the governing body should not be about specific child protection cases, but should review the safeguarding policies and procedures. It is good practice for the nominated governor and the DSP to present the report together"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the Welsh Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners. This will be carried out by the (*insert name of governor group/committee*) whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor[3]

to include:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant *governors group/meeting*
- *membership of the school Online Safety Group*
- *occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The online safety lead will:

- lead the Online Safety Group

[3] It is suggested that the role may be combined with that of the designated governor for safeguarding. In other settings this may be the management committee person for child protection

- work closely on a day-to-day basis with the Designated Safeguarding Person (DSP), where these roles are not combined
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents[4] and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/ governors/ parents/ carers/ learners
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team.
- liaises with the local authority/relevant body.

Designated Safeguarding Person (DSP)

Keeping Learners Safe states:

> 2.14. "The headteacher/principal must appoint the appropriate number of DSPs and deputy DSPs for their education setting and should ensure the DSP:
>
> - is given sufficient time and resources to carry out the role effectively, which should be explicitly defined in the postholder's job description
> - has access to the required levels of training and support to undertake the role, including online safety training
> - has time to attend and provide reports and advice to case conferences and other inter-agency meetings as required

[4] The school will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the online safety lead or another member of staff, e.g. headteacher/senior leader/Designated Safeguarding Person/class teacher/head of year, etc.

- has the appropriate IT equipment to carry out the role effectively."

The Designated Safeguarding 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 (See 'Personal data policy' in the Appendix.)
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

Curriculum Leads

The Keeping Learners Safe safeguarding audit tool suggests:

> "The curriculum should support existing policy within the education setting on important issues and provide sufficient information on managing risk, e.g. in: sex and relationships; drug, alcohol and tobacco education; accident prevention; anti-bullying; online safety; extremism and radicalisation."

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through (amend/delete as relevant):

- a discrete programme
- the Digital Competence Framework
- relationships and sexuality education
- Health and Wellbeing area of learning and experience
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA), and that this is reviewed regularly

- they immediately report any suspected misuse or problem to *(insert relevant person)* for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners, parents and carers should be on a professional level *and only carried out using official school systems and devices*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and 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 that are 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to Live-streaming and video-conferencing: safeguarding principles and practice guidance, which outlines key considerations to ensure safe practice when live-streaming.
    - Keeping Learners Safe (Paragraph 7.6) states: "Safeguarding is an integral principal of digital learning and the safety and welfare of learners must take precedence over all other considerations. Safeguarding must be integral to the delivery of live-streamed lessons to ensure learners are appropriately protected."
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The network manager/technical staff (or local authority/managed service provider) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy in order to carry out their work effectively in line with school policy
- 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, Welsh government via the Education Digital Standards or other relevant body
- users may only access the networks and devices through a properly enforced password protection policy

- 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 technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- *the filtering policy (*if one exists*), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person* (see appendix 'Technical Security Policy template' for good practice).
- *(if present) monitoring software/systems are implemented and updated as agreed in school or education technology support partner policies*

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (this should include personal devices – where allowed), and this is reviewed annually.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- will be expected to know and follow school Online Safety Policy
- 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.

Enhancing digital resilience in education: An action plan to protect children and young people online (November 2022) states:

> *"We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business."*

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- *providing opportunities for parents and carers to improve their understanding of online safety through parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns and literature (amend as relevant)*

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school*
- *the use of their children's personal devices in the school (where this is allowed)*

Community users

Community users who access school systems/website/Hwb/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. (A community user's acceptable use agreement template can be found in the appendices).

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

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.

The Online Safety Group has the following members (amend as appropriate):

- online safety lead
- Designated Safeguarding Person
- senior leaders
- online safety governor

- teacher and support staff members
- learners
- parents/carers
- community representatives

Members of the Online Safety Group (or other designated group) will assist the Online Safety Lead (or other relevant person) with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school web filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage of the Digital Competence Framework
- reviewing network/web filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, recent trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers 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.

Professional Standards

There is an expectation that national professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (to be described)
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed.

The Online Safety Policy and appendices define acceptable use at the school. Within the appendices there are acceptable use agreements for:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters/splash screens around the school. *Learner groups (to be described) are encouraged to suggest child friendly versions of the rules.*
- staff /volunteer AUAs will be agreed and signed by staff and volunteers
- parent/carer AUAs inform them of the expectations of acceptable use for their children and seek permissions for digital images, the use of cloud systems etc.
- community users that access school digital technology systems will be required to sign an AUA.

The acceptable use agreements will be communicated/re-enforced through: (amend as appropriate)

- student handbook
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

Schools will need to discuss and agree which activities are acceptable/unacceptable. This will vary with the size/structure of the school and the ages of the learners. It is recommended that the school should discuss and agree on these activities and to complete the following tables as guidance for members of the school community:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online	Any illegal activity for example:					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated nude and semi-nude images (sometimes referred to as 'sexting') - Sharing nudes and semi-nudes: Responding to incidents and safeguarding children and young people.					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – read more about this: NCA Cyber Choices Programme					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				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	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Staff and other adults	Learners

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal email in school, or on school network/wi-fi								

Use of school email for personal emails								

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table.

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

- when communicating in a professional capacity, staff should ensure that the communication tools they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (email, social media, learning platform, etc.) must be professional in tone and content. *Personal email addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a 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
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.*

Reporting and responding

The school has in place procedures for identifying and reporting cases, or suspected cases, of online safeguarding issues/incidents and understands that because of our day-to-day contact with children our staff are well placed to observe the outward signs of these issues.

We ensure that every member of staff and every governor knows that they have an individual responsibility for reporting and that they are aware of the need to be alert to signs of abuse and neglect, and know how to respond to a learner who may disclose such issues.

We also understand that reporting systems do not always respond to the needs of learners and that we need to identify issues and intervene early to better protect learners. *In order to do this, schools should "Recognise that peer-on-peer sexual harassment is highly prevalent in the lives of young pupils and adopt a whole-school preventative and proactive approach to dealing with it." (Estyn, 2021)*

Schools should understand that online behaviours change, there is a risk that by drawing attention to certain behaviours, schools may inadvertently push children and young people towards the very content from which they are trying to protect them. Therefore, particular care should be given to the manner in which information is shared by schools about online challenges and hoaxes. More information is available in this guidance on Hwb.

The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

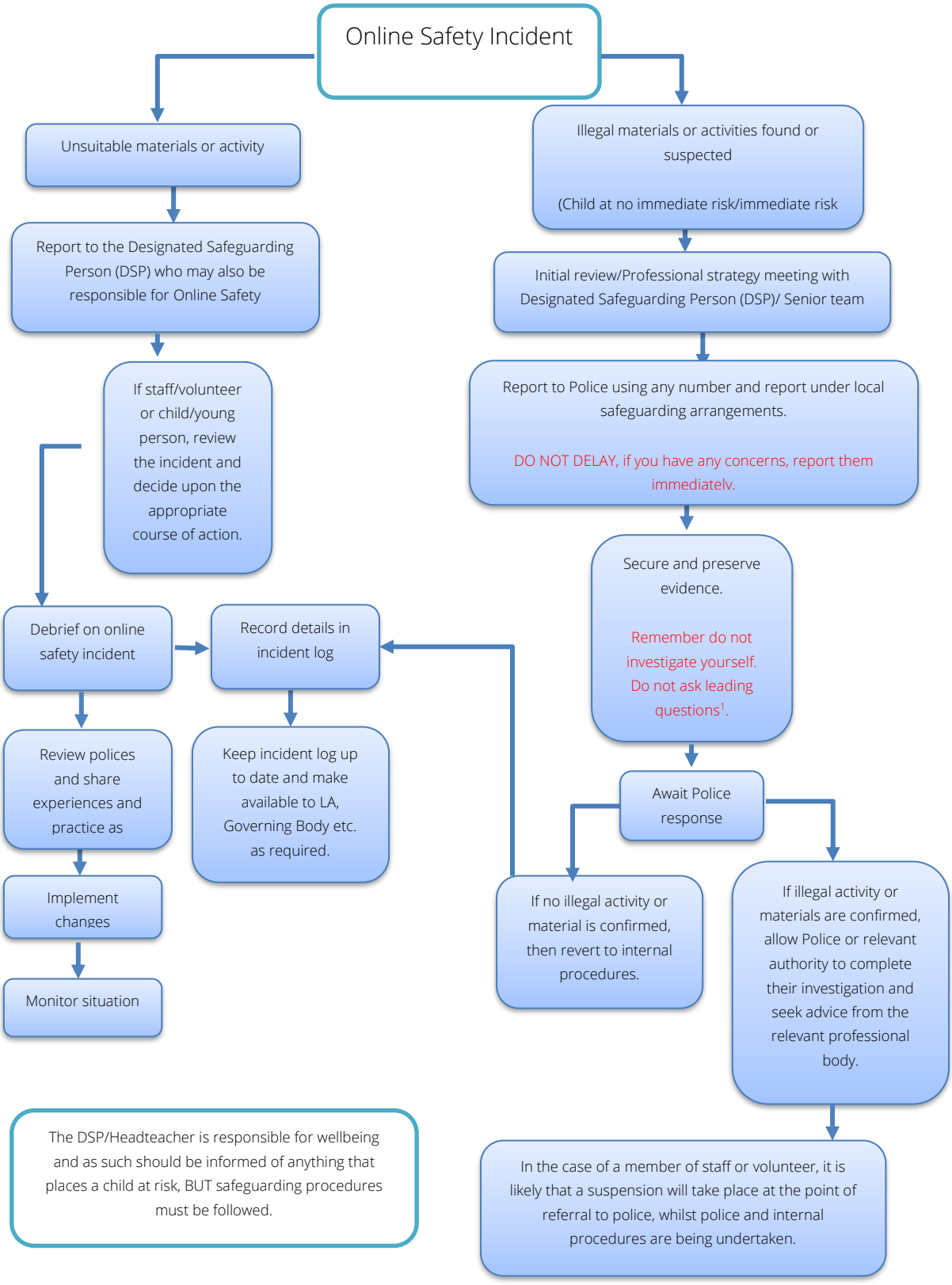
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. (Schools may wish to consider the use of online/anonymous reporting systems, which can be used by all members of the school community)
- all members of the school community will be made aware of the need to immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm (see flowchart and user actions chart below), the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents 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.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should

illegal activity be subsequently suspected). 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 above).
- 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 (as relevant)
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those who are reporting or are affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident
Unsuitable materials or activity
Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as
Keep incident log up to date and make available to LA, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
(Child at no immediate risk/immediate risk
Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior team
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediatelv.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
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, whilst police and internal procedures are being undertaken.
The DSP/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

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: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		X	X						
Corrupting or destroying the data of other users.		X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X				
Unauthorised downloading or uploading of files or use of file sharing.		X	X						

Using proxy sites or other means to subvert the school's filtering system.		X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident.		X	X	X	X				
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X						
Unauthorised use of digital devices (including taking images)		X	X	X					
Unauthorised use of online services		X	X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X						
Continued infringements of the above, following previous warnings or sanctions.		X	X						

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.		X						
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.		X	X					
Using proxy sites or other means to subvert the school's filtering system.		X	X					
Unauthorised downloading or uploading of files or file sharing.		X	X					
Breaching copyright or licensing regulations.		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					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.		X	X	X				

Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers		X	X					
Inappropriate personal use of the digital technologies e.g. social media / personal email.		X	X					
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner.		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 or the ethos of the school.		X	X					
Failing to report incidents whether caused by deliberate or accidental actions.		X	X					
Continued infringements of the above, following previous warnings or sanctions.		X	X					

Education

Online Safety Education Programme

Enhancing digital resilience in education: An action plan to protect children and young people online states:

> "With so many aspects of our lives now entwined with using technology in an online world, supporting our children and young people to be digitally resilient is fundamental. Digital resilience encapsulates the need to develop knowledge, skills and strategies in order for children and young people to:
>
> - manage their online experience safely and responsibly while protecting their digital identity
> - identify and mitigate risks to stay safe from harm online

- understand the importance of using reliable sources and employing critical thinking skills to identify misinformation
- seek help when they need it
- learn from their experiences and recover when things go wrong
- thrive and benefit from the opportunities the internet offers."

> "Building digital resilience within our children and young people prepares them to become well-rounded and balanced citizens that recognise the impact of their actions. Ensuring our children and young people use technology responsibly to foster a culture where mental and physical health is not adversely affected by the internet is crucial.
>
> Supporting the social and cultural development of our children and young people, including promoting values such as tolerance and respect for others in all environments, is another overarching objective, which we set out to achieve through our online safety education activities."

Guidance for education settings on peer sexual abuse, exploitation and harmful sexual behaviour states:

> "Young people increasingly experience abuse and exploitation online and/or digitally. This will be more difficult for education settings to identify, as some of it is likely to occur outside schools and colleges. However, it is important to consider the impact of this on young people's offline lives."

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited

- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

Contribution of Learners

Keeping Learners Safe states:

"How safe do learners feel? The United Nations Convention on the Rights of the Child (UNCRC) sets out that children have a right to be safe and protected from harm, and have the right to express their opinions and participate in decision-making. In accordance with the UNCRC, the best way to understand how safe an education setting feels to learners is to ask them and observe how they and staff interact."

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors (or similar groups)*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

- a planned programme of formal online safety, cyber security and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify online safety as a training need within the performance management process*
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- *the Online Safety Lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe*

online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations

- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

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:

- Hwb training – Online safety for governors
- attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

Schools should consider providing all governors with a Hwb account in order to use the secure tools and services available e.g. Microsoft Outlook, Teams etc as well as appropriate application training. This would negate the need for governors to use personal email accounts, thereby reducing the risk to data.

Families

Enhancing digital resilience in education: An action plan to protect children and young people online states:

> "Building digital resilience in our children and young people also depends on the resilience of our families and communities. We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business."

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 seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform, Hwb*
- *high profile events/campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, The UK Safer Internet Centre, Childnet International (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority*

Adults and Agencies

The Enhancing digital resilience in education: An action plan to protect children and young people online draws upon the self-review information schools in Wales record in the 360 safe Cymru tool. This data highlights that schools showing the strongest performance, amongst other indicators,

'ensure that parents and carers receive these important online safety messages, often through the learners themselves sharing the messages learned in school. The school will also share their good practice with the wider community and other schools and will make use of the valuable community resources available to them from agencies such as the police'.

Drawing on this intelligence, the school will provide opportunities for local community groups and members of the wider 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 and online safety
- online safety messages targeted towards families and relatives.

- the school will provide online safety information via their learning platform, website, and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (for early years settings please refer to the Online Safety Toolkit for early years practitioners)

The school recognises the support and advice that may be provided by external groups and agencies and values their contribution to school programmes and events.

The school is committed to sharing its good practice with other schools and education settings.

Technology

The school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures that are in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Keeping Learners Safe states:

> 7.7. "It is critical that web-filtering standards are fit for purpose for twenty-first century learning and teaching, allowing the access schools require while still safeguarding children and young people. Governing bodies should ensure appropriate filters and appropriate monitoring systems are in place and refer to web filtering standards as part of the Education Digital Standards for schools in Wales. The standards seek to support schools to provide a safe, responsible and supportive environment to learn in, and prevent access to inappropriate or harmful content.

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government Education Digital Standards - Web filtering and the UK Safer Internet Centre Appropriate filtering. (The school will need to decide on the merits of external/internal provision of the filtering service – see Technical Security Policy Template in the Appendix).
- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police

assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

- there are established and effective routes for users to report inappropriate content and this is acted upon in a timely manner by the Designated Safeguarding Person whilst adhering to the Wales Safeguarding Procedures
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age appropriate search engines e.g. Google safe search, SWGfL Swiggle
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- filtering logs are reviewed frequently and alert the school to breaches of the filtering policy, which are then acted upon.
- *Devices that are provided by the school have school-based filtering applied irrespective of their location.*
- *where personal mobile devices are permitted for use, there is clear separation between the school network filtering and the associated guest network filtering.*
- *the system manages access to content through non-browser services (e.g. apps and other mobile technologies)*

If necessary, the school will seek advice from, and report issues to, the Report Harmful Content site.

Monitoring

The school monitors network traffic at a local level, follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

- a staff lead who is responsible for managing the monitoring strategy and processes.
- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- monitoring and filtering logs are regularly analysed and breaches are reported to senior leaders
- monitoring enables alerts to be matched to users and devices.
- there is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*

Users are made aware, through the acceptable use agreements, that monitoring takes place. (schools may wish to add details of the monitoring programmes that are used).

Technical Security

The school has a clear technical security policy and systems will be managed in ways that ensure that the school meets recommended technical requirements

- system security training is available for all staff users
- there will be regular reviews and audits of the safety and security of school technical systems and of the school's technical support
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud and these are resilient by design (this is good practice in helping to prevent loss of data from ransomware attacks)
- A documented access control model should be in place, clearly defining access rights to school systems and devices. This should be reviewed annually. all users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Sharing of passwords or username and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Cardidd County Council who will keep an up-to-date record of users and their usernames.
- the master account passwords for the school systems are kept in a secure place, e.g. school safe. It is recommended that these are secured using two factor authentication for such accounts
- systems are in place for the recovery and resetting of passwords
- passwords should be long.

- Only if necessary, records of learner usernames and passwords for Foundation Phase learners may be kept in an electronic or paper-based form, but they must be securely stored when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Cardiff County Council is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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.
- systems and programme software are regularly updated with security patches
- 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 agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- an agreed device management policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail)
- encryption is used for the transfer of sensitive or vulnerable data and on school managed devices
- dual-factor authentication is used for sensitive data or access outside of a trusted network

Devices

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the 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 email 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 devices 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 devices should be an integral part of the school's online safety education programme.

In preparing a devices 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.

Before implementing a devices policy, schools must undertake a Data Protection Impact Assessment (DPIA) (the page includes a link to a sample DPIA) . Should this identify a high risk to personal data that cannot be controlled then the school is obliged to inform the ICO of this residual risk and are recommended not to proceed with this approach. The ideal situation is for schools to identify a suitable remote access approach (such as a VPN) that provides staff with safe and secure access to personal data.

A range of device implementations is possible.

For further reading, please refer to the Welsh Government Education digital guidance for schools and Bring your own device guidance

A more detailed devices policy template can be found in the Device Management Policy Template Appendix. The school may instead choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate devices policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered is included below.

- The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of devices.

- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems).

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[5]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes/No[6]	Yes/No[8]	Yes/No[8]
Full network access	Yes	Yes	Yes			
Internet only						
No network access						

Aspects that the school may wish to consider and include in their Online Safety Policy, devices policy or acceptable use agreements should include the following:

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school (note the need for some areas to be clearly identified as mobile free zones)*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*

[5] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[6] The school should add below any specific requirements about the use of mobile/personal devices in school.

- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

Personal devices

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *levels of access to networks/internet (e.g. access, or not, to internet/guest wi-fi/network)*
- *network/broadband capacity*
- *technical support (this may be a clear statement that no technical support is available)*
- *filtering of the internet connection to these devices and monitoring the access*
- *management of software licences for personally owned devices. (the national Microsoft licensing deal through Hwb allows teachers and learners to install core Microsoft applications on personal devices)*
- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

Social media

With the popularity of use of all types of social media for professional and personal purposes, a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing

any material online. The Practices and principles for schools' use of social media guidance on Hwb provides further information.

Expectations for teachers' professional conduct are set out by the Education Workforce Council (EWC) 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 follow the professional conduct set out by the Education Workforce Council (EWC) and respect learners, their families, colleagues and the school.

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
- providing education/training on social media use including; acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- having in place clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- provision of guidance for learners, parents/carers

School staff ensure that:

- no reference is made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

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

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school will effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

The social media policy template in Appendix C4 provides more detailed guidance on the school's responsibilities and on good practice.

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/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 (select/delete as appropriate):

- should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance and Keeping Learners Safe para 7.6
- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes*
- *care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images*

- *learners' full names will not be used anywhere on a website or blog, particularly in association with photographs*
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy

images will be securely stored on the school network in line with the school retention policy and in accordance with the Data Protection Act 2018

- *learners' work can only be published with the permission of the learner and parents/carers.*

Online safety messaging

The school communicates with parents/carers and the wider community and promotes the school through (amend as necessary):

- Public-facing website
- Social media
- Online newsletters
- Other

The school website is managed/hosted by (insert details). The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Security

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

The school:

- has a Data Protection Policy. (see appendix for template policy)
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- 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. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an Iinformation Asset Register (IAR) in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the IARlists 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
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject. For example one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them

- carries out Data Protection Impact Assessments (DPIAs) where necessary e.g. 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
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools should consider using the Wales Accord on Sharing Personal Information (WASPI) toolkit to support regular data sharing between data controllers
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- as a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking 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:

- data will be encrypted and password protected.
- device will be password protected. (be sure to select devices that can be protected in this way)
- device will be protected by up to date virus and malware checking software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they: (schools may wish to include more detail about their own data/password/encryption/secure transfer processes)

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Cyber Security

Enhancing digital resilience in education: An action plan to protect children and young people online describes cyber security as:

> "The term used to describe how both individuals and organisations can reduce the risk of cyber attacks. Cyber security's main purpose is to ensure the technology we use (devices such as computers, tablets and smartphones) and the services we access online are protected from the risk posed by cyber crime including theft for gain such as ransomware attacks and seeking competitive advantage, or malicious damage intended to disrupt an organisation's ability to operate effectively. We store large amounts of personal and organisational information on devices and services and preventing unauthorised access to this information is critical."

The 'Cyber security in schools: questions for governing bodies and management committees' guidance produced by the National Cyber Security Centre (NCSC) working with Welsh Government aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security

conversation between the governing body and school leaders, with the governing body taking the lead.

The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the school has adopted and made use of the relevant Hwb Network and Data Security Standards
- the school, in partnership with their education technology support partner, has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school, in partnership with their education technology support partner, has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff receive training on the common cyber security threats and incidents that schools experience

the school has a business continuity and incident management plan in place that includes IT and these wider services.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from Hwb.

The 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 template and of the 360 safe Cymru online safety self-review tool:

Acknowledgements:

- Members of the SWGfL Online Safety Group
- Representatives of Welsh local authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use. Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in March 2024. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2024

Appendices

A1 Learner Acceptable Use Agreement template – for older learners 48
A2 Learner Acceptable Use Agreement Template – for KS2 52
A3 Learner Acceptable Use Policy Agreement Template – for younger pupils 55
A4 Parent/Carer Acceptable Use Agreement Template and permission forms 56
A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template 64
A6 Acceptable Use Agreement for Community Users Template 68
A7 Online Safety Group Terms of Reference template 70
A8 Responding to incidents of misuse – flow chart 73
A9 Record of reviewing devices/internet sites 74
A10 Reporting Log 75
B1 Training Needs Audit Log 76
C1 Technical Security Policy Template (including filtering and passwords) 77
C2 Personal Data Advice and Guidance 87
C3 Device Management Policy Template (including Bring Your Own Device) 102
C4 Social Media Policy Template 107
Legislation 113
Links to other organisations or documents 119

A1 Learner Acceptable Use Agreement template – for older learners

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final acceptable use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final document will be more concise. Schools will need to decide on the suitability of the statements/language used and may wish to amend these in light of the age/abilities of the learners.

School policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These 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. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that children and young people will have good access to digital technologies, 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.

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 the 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 a trusted adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable to a trusted adult 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 not use them for personal or recreational use unless I have permission
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so. (schools should amend this section to take account of their policy on each of these issues)

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files without 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 not take or distribute images of anyone without 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 devices (mobile phones/USB devices etc.) in the school if I have permission (schools should amend this section in the light of their mobile devices policies). I understand that if I do use my own devices 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, to the relevant staff member, any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails (unless I know and trust the person/organisation who sent the email) 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).

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 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 the 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 may be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

The school will need to decide if they will ask learners (and/or) their parents/carers to sign the AUA or whether it is sufficient to just make it clear that these rules should be followed and to re-enforce them through the year. The form below is provided for those schools that wish to have them signed.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to confirm that you have read, understood and agree to the rules included in the learner acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document in the Parent/Carer AUA)). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

A2 Learner Acceptable Use Agreement Template – for KS2

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final acceptable use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their school policies. Schools will need to decide on the suitability of the statements/language used and may wish to amend these in light of the age/abilities of the learners.

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and the internet, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me

- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do. (schools may wish to add anything that would not be allowed e.g. online games, file sharing etc.)

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission (schools should amend this section in the light of their mobile devices policies). If I am allowed, I still have to follow all the other school rules if I use them.
- I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).
- 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 is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

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

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) *loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.*

The school will need to decide if they will ask learners (and/or) their parents/carers to sign the AUA or whether it is sufficient to just make it clear that these rules should be followed and to re-enforce them through the year. The form below is provided for those schools that wish to have them signed.

Learner Acceptable Use Agreement Form

Please complete the sections below 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. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document in the Parent/Carer AUA). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

A3 Learner Acceptable Use Policy Agreement Template – for younger pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult 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.

Signed (child): .....

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

Signed (parent): .....

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the parent/carer acceptable use agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

A4 Parent/Carer Acceptable Use Agreement Template and permission forms

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies provide 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 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 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 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 learners 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 work. (Schools will need to decide whether or not they wish parents to sign the acceptable use agreement on behalf of their child)

Permission Form

Parent/Carers Name:..... **Name(s) of Learners**.....

As the parent/carer of the above learners, I give permission for my child to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my child 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 child 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 the school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and 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 child's activity on the 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.

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

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....

Date: .....

When complete, ensure the information on this form is recorded in the school database.

When complete, this page should be stored in a secure location for the duration of:

Use of Digital/Video Images

There are certain activities where the school do not use consent as the basis for processing your child's data. We take photographs/videos of the children for the purposes of recording and tracking pupil progress under the [*e.g. Education Act 1996*] and compiling evidence for assessment purposes. These are kept in secure locations within the school and destroyed in line with our retention policy. We may also need to share these files with third parties, such as [*Insert professionals/third parties who may be a recipient or contributor, if any*]. Further details can be found in the school privacy notice.

On other occasions the school may wish to publish photographs and/or video footage of pupils in public documents such as the school prospectus, our social media pages (e.g. Twitter) and website, on display around the school, and in community publications such as local newspapers. All images are published with the strictest regard for safeguarding and child protection, and only with your consent.

The school will comply with data protection laws and request parent's/carers permission before publishing images of members of the school. We will also ensure that when images are published the learner cannot be identified using their names.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, please contact the school.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to how it will be used and stored:

This form (electronic or printed)	The images
The school will retain the consent form for the period of 1 academic year. Consent for the publication of photographs/images will be renewed on an annual basis.	Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
	Who will have access to the images.
	Where the images will be stored.
	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. Parents/Carers should note that websites can be viewed throughout the World, and not just in the United Kingdom where UK/EU data protection law applies. Images and information can no longer be controlled by the school when copied from the website.

Digital/Video Images Permission Form

Parent/Carers Name:..... Name(s) of Learner(s):.....

Description of the use of Photographs or Images	Please Tick	
I agree for photographs/videos to be taken of my child during school activities for use on display boards or walls around the school.	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities for use within school printed publications.	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities for use on school digital channels (e.g. websites, social media).	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities and used in local or national media (e.g. newspapers or television appearance).	☐ Yes	☐ No

OR

I do not wish any photographs/videos to be taken of my child for the purposes outlined above.	☐ Yes	☐ No

Signed: .....

Date: .....

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by Data Protection Laws). However, to respect everyone's privacy (and in some cases protection) these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Use of Cloud Systems

In Wales, all learners have access to Hwb through a personalised account. In order for an account to be created, personal data is shared between the school and Hwb. The use of personal data in this manner is considered to be a public task, for the purposes of data protection. This means that consent is not required in order for a learner to have a Hwb account and access to the tools and services on this platform. More details can be found in the Hwb trust centre.

Schools that use other cloud hosting services should assess the risk of sharing personal data with any other third party and should identify the correct lawful basis for this data sharing. It is likely that parent/carer consent may be required in order to create an account. Schools should consider the impact of relying on consent as the lawful basis if the service is regarded as essential to providing education. If consent is withdrawn and access to the service no longer possible, the school should consider if this would have a negative impact on the learners' education?

Schools may wish to include a simple form to collect any necessary permission here.

Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as learners do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a Data Privacy Impact Assessment and is confident that the use of such technologies is effective and justified in a school context. Please see below for more information:

As the school is collecting special category personal data and *delete as appropriate* sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared
Where this form will be stored.	Who the data will be shared with
How long this form will be stored for.	Who will have access to the data.
How this form will be destroyed.	Where the data will be stored.
	How long the data will be stored for.
	How the data will be destroyed.
	How consent to process the biometric data can be withdrawn.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a learner's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parent/Carers Name:.....**Name(s) of Learner(s)** .....

Where your child is over 13 years of age, we recommend that you complete this form with them, as learners may be able to decide how their data may be used in certain circumstances.

As the parent/carer of the above learner(s), I agree to the school using biometric recognition systems, as described above.	Yes/No
I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school	Yes/No

Signed:.....

Further guidance

- Each parent of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This needs to be in writing.
- A child aged over 13 can object or refuse to participate in the processing of their biometric data regardless of parents' consent.
- Schools must provide reasonable alternative means of accessing services for those learners who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the learner attends the school, but new permission is required if there are changes to the biometric systems in use.

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUA will be more concise.

School Policy

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

This acceptable use policy 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 technology in their everyday work.

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

Acceptable Use Policy 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. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the children and young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of the school (schools should amend this section in the light of their policies which relate to the use of school systems and equipment out of the 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 systems:

- I will not access, copy, remove or otherwise alter any other user's files, without 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 policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) 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 the school in accordance with school policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with learners and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications)
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- When I use my personal mobile devices 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. (schools should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal email addresses on the school ICT systems. (schools should amend this section in the light of their email policy – some schools will choose to allow the use of staff personal email addresses on the premises).
- 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, terrorist or extremist material, 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 not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools should amend this section in the light of their policies on installing programmes/altering settings)
- 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 documents containing personal 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.

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 policy applies not only to my work and use of school digital technology equipment in the 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 (schools should amend this section to provide relevant sanctions as per their behaviour policies) 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 the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A6 Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure that:

- community users will be responsible and stay safe while using school systems and devices and will be protected from potential harm in their use
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable/cause any damage to school equipment, or the equipment belonging to others.

- I will immediately report equipment/software damage/faults, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- I will not download or distribute copies of work protected by copyright (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

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

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

Name: .....

Signed: .....

Date: .....

A7 Online Safety Group Terms of Reference template

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 of 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 one member of staff may hold more than one of these posts):
[add/delete where appropriate]

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety lead (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT 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 committee 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 Online Safety 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 Online Safety 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 those 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 Lead (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/VLE/newsletters
    - online safety events
    - Safer Internet Day (SID) which is held on the second Tuesday in February every year
    - other methods
- To ensure that monitoring is carried out of internet sites used across the school.
- 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.

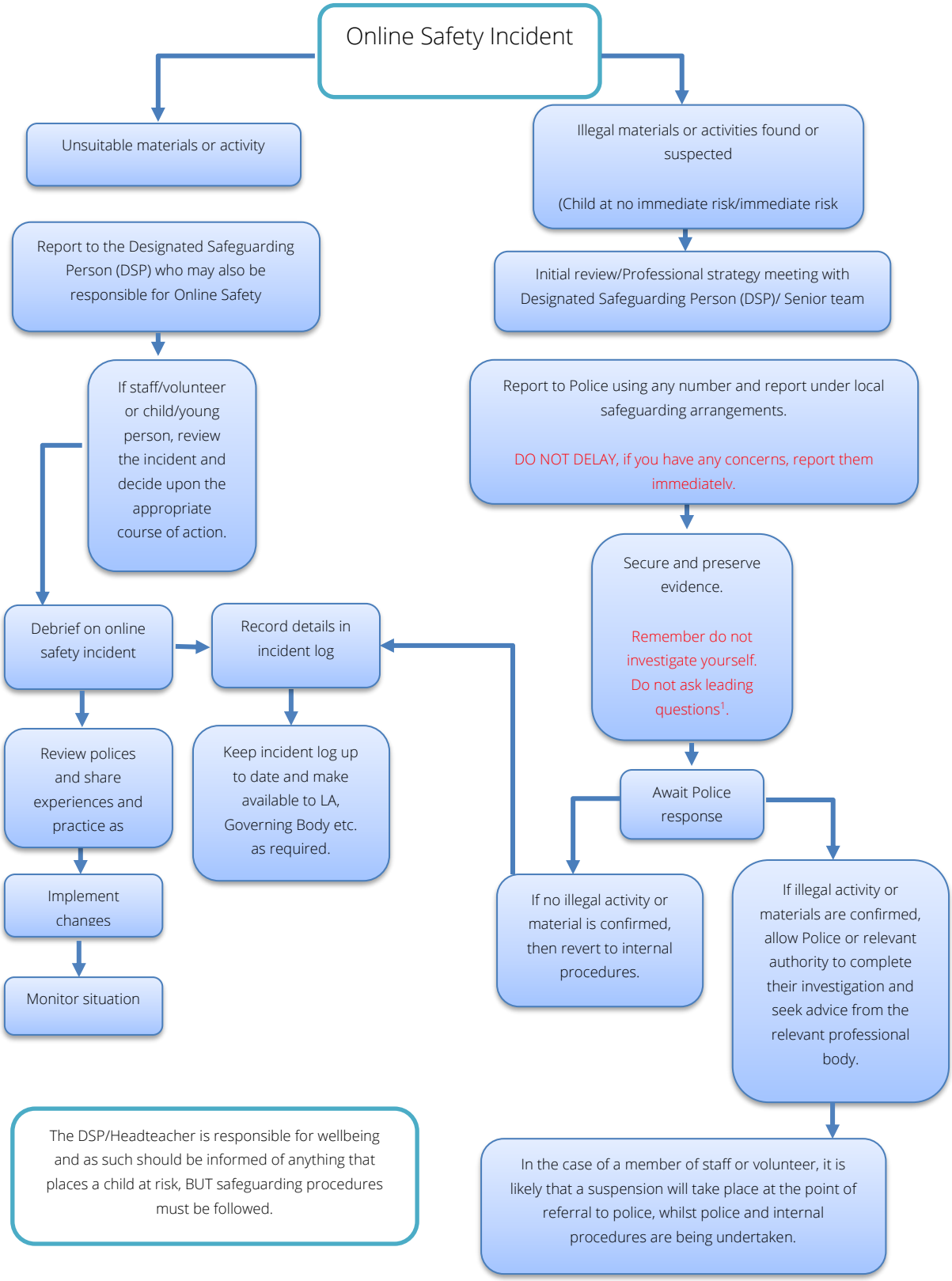
The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT): .....

Date: .....

Date for review: .....

A8 Responding to incidents of misuse – flow chart



A9 Record of reviewing devices/internet sites

(responding to incidents of misuse)

School: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

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

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

A10 Reporting Log

School: .....

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

B1 Training Needs Audit Log

School: .....

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

C1 Technical Security Policy Template (including filtering and passwords)

Suggestions for use

Within this template sections which include information or guidance are shown in BLUE. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in italics it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL Online Safety Group that these would be an essential part of a school Online Safety Policy.

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another user's files (other than that allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.
- Logs are maintained of access by users and of their actions while users of the system.
- There is effective guidance and training for users.
- There are regular reviews and audits of the safety and security of school devices.
- User activity is monitored and filtered, and that adequate processes are in place to detect and respond to incidents.
- There is oversight from senior leaders and these have impact on policy and practice.

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all of the online safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school's online safety policy/acceptable use agreements). The school should also check their local authority/other relevant body policies and guidance on these technical issues. Schools should also consider the guidance available in the Hwb Support Centre.

Responsibilities

The management of technical security will be the responsibility of (insert title) (schools will probably choose the Network Manager/Technical Staff/Head of Computing or other relevant responsible person)

Technical Security

Policy statements

The school will be responsible for ensuring that their infrastructure 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 receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (if not managed by the Local Authority, these may be outlined in local authority/other relevant body technical/online safety policy and guidance).
- 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.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, end-user devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level).
- All users will have clearly defined access rights to school technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the Online Safety Group.*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their logon details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below).
- (insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.)
- *Device security and management procedures are in place* (where devices are allowed access to school systems). (Schools may wish to add details of the device security procedures that are in use).

- *School/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.* (Schools may wish to add details of the monitoring programmes that are used)
- *Remote management tools are used by staff to control workstations and view users activity.*
- *An appropriate system is in place* (to be described) *for users to report any actual/potential technical incident to the Online Safety Lead/network manager/technician (or other relevant person, as agreed).*
- An agreed policy is in place (to be described) for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school technical system.
- *An agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programs on school devices by users.*
- *An agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.*
- An agreed policy is in place (to be described) regarding the use of removable media (e.g. USB pen drive/CDs/DVDs) by users on school devices (see school personal data policy template in the appendix for further detail).
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats such as viruses, malware, and randomsomware..
- Personal data cannot be sent over the internet or taken off the school site unless encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail.)

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and virtual learning platform). Where sensitive data is in use – particularly when accessed on personal devices – schools may wish to use more secure forms of authentication e.g. two factor authentication.

Further guidance can be found from the Hwb Support Centre, National Cyber Security Centre and SWGfL "Why password security is important".

Policy Statements:

- These statements apply to all users.
- All school networks and systems 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 Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).

- All users (learners and staff) have responsibility for the security of their username and password, must not allow other users to access the systems using their logon details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by xxxxx (insert name or title) (see section on password generation in technical notes) who will keep an up-to-date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the school.

Staff should not use or encourage the use of the same or similar passwords for multiple users. Passwords should be unique for each user.

- Passwords must not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on the first login to the system.
- *The school may wish to recommend to staff and learners (depending on age) that they make use of a password manager that can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.*
- *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

Learner passwords:

Primary schools will need to decide at which point they will allocate individual usernames and passwords to learners. Schools should use individual logons wherever possible, in the case of Hwb these may already have been provisioned for you. Whilst schools may choose to use class logons for services other than Hwb, these should be implemented with caution as schools need to be aware of the risks associated with not being able to identify any individual. Use by learners in this way should always be supervised and members of staff should never use a class logon for their own network/internet access. Schools should also consider the implications of using whole class logons when providing access to virtual learning environments and applications, which may be used outside school.

- Records of learner usernames and passwords for foundation phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- Users will be required to change their password if it is compromised. Some schools may choose to reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process. (Note: passwords should not be regularly changed but should be secure and unique to each account.)
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Schools may wish to add to this list for all or some learners any of the relevant policy statements from the staff section above.

Notes for technical staff/teams

- Where possible, each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level.
- Consideration should also be given to using two factor authentication for administrator accounts.
- An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. (A school should never allow one user to have sole administrator access)
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated* by xxxxx (insert title) (schools may wish to have someone other than the school's technical staff carrying out this role e.g. an administrator who is easily accessible to users). *Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by* xxxxx (insert title) *to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated* by (the responsible person) *to ensure that the new password can only be passed to the genuine user* (the school will need to decide

how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)

- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expire after use. *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety Policy and password security policy
- through the acceptable use agreement

Learners will be made aware of the school's password policy:

- in lessons (the school should describe how this will take place)
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person (insert title) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools need to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation
- Whether to introduce differentiated filtering for different groups/ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used

Keeping Learners Safe requires schools to have "appropriate filtering". Guidance can be found on the UK Safer Internet Centre site and the Welsh Government Web filtering standards.

Schools may wish to test their filtering for protection against illegal materials at: SWGfL Test Filtering

Responsibilities

The responsibility for the management of the school's filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- be logged in change control logs
- be reported to a second responsible person (insert title):
- *either… be reported to and authorised by a second responsible person prior to changes being made* (recommended)
- *or… be reported to a second responsible person* (insert title) *every X weeks/months in the form of an audit of the change control logs*
- *be reported to the Online Safety Group every X weeks/months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any applications that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Either - The school maintains and supports the managed filtering service provided by their Internet Service Provider* (or other filtering service provider)
- *Or – The school manages its own filtering service* (N.B. If a school decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the Headteacher would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff/learners)
- *The school has provided enhanced/differentiated user-level filtering through the use of the* (insert name) *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
- *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *School owned mobile devices should be subject to the same filtering standards when used on external networks as they do when on the school system.*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (insert name or title) (N.B. an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in the school or by an external filtering provider).
- the grounds on which they may be allowed or denied (Schools may choose to allow access to some sites e.g. social networking sites for some users, at certain times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- any audit/reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring

Some schools supplement their filtering systems with additional monitoring systems. If this is the case, schools should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network/equipment as indicated in the school Online Safety Policy and the acceptable use agreement. *Monitoring will take place as follows:* (details should be inserted if the school so wishes).

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- the second responsible person (insert title)
- Online Safety Group
- Online Safety Governor/Governors committee/Management Committee member for child protection
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Further Guidance

Schools may wish to seek further guidance. The following is recommended:

Welsh Government – Keeping Learners Safe

Recommended filtering standards for schools in Wales

Hwb Support Centre

Under the Prevent duty legislation, schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (for more information see Hwb - Keeping Communities Safe: Understanding the Prevent Duty in Wales).

UKSIC - "Appropriate Filtering"

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

C2 Personal Data Advice and Guidance

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school is encouraged to seek their own legal counsel when considering their management of personal data.

Data Protection Law: a legislative context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union (EU) General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act (DPA) 2018 replaced the Data Protection Act 1998.

The EU GDPR has been incorporated into UK law as the UK GDPR. The 'UK GDPR' and the DPA 2018 means the UK will have the independence to keep the framework under review. Therefore, the key principles, rights and obligations remain the same. However, there are implications regarding the rules for transferring personal data between the UK and the European Economic Area (EEA). In June 2021 the EU adopted an adequacy decision for unrestricted data flows between the UK and the EU until June 2025. Essentially, this means that all the regulations that were brought about in 2018 remain the correct framework to operate within and schools should continue to ensure that data transfers take place in a compliant and lawful manner.

In this document the term "data protection law" refers to the legislation applicable to data protection and privacy as applicable in the UK.

Does the data protection law apply to schools?

In short, yes. All schools process personal data and are considered a separate 'data controller' for the purposes of data protection.

Personal data is "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is one who can be identified, directly or indirectly, by reference to:

- an identifier such as a name, an identification number, location data, an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Some types of personal data are known as 'special categories of personal data' and include the following:

"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"

The school must identify both a lawful basis (Article 6 of the UK GDPR) and a separate condition for processing special category data (Article 9 of the UK GDPR). These should be decided prior to any processing taking place, and further guidance is available on the Information Commissioner's Office (ICO) website

The ICO's powers are wide ranging in the event of non-compliance and schools must be aware of the huge impact that a fine or investigation will have on resources, finances and in the wider community, for example, in terms of trust.

Data protection law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes ("purpose limitation");
c) adequate, relevant and limited to what is necessary ("data limitation");
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation"); and
f) processed in a manner that ensures appropriate security of the personal data

An overall principle of accountability requires the school to be responsible for and demonstrate compliance with data protection law.

Data protection law requires the school to always have a **lawful basis for processing** personal data. These can be summarised as:

(a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)

(b) 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.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) 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.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

No single basis is 'better' or more important than the others and which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Data mapping to identify personal data, data subjects and processing activities

The school and its employees will collect and or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a data map of these activities. These inform privacy notices and help put security measures in place to keep personal data secure, including steps to avoid a breach, and ensure Data Sharing Agreements or Data Processing Agreements (i.e. contracts) are in place with the suppliers or contractors.

The data map should identify what personal data is held in digital format or on paper records in a school, where the information is stored, why it is processed, and how long it is retained.

In a typical data map for a school, the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors: personal data of names, addresses, contact details
- Learners: curricular / academic data (e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports)
- Staff and contractors: professional records (e.g. employment history, taxation and national insurance records, appraisal records and references, health records)

The ICO have advice and guidance on keeping a Record of Processing Activities.

The school will need to identify appropriate lawful process criteria for each type of personal data, and if this is not possible, such activities should be discontinued.

A school can use the public task lawful basis if processing takes place to perform an official task as set down in UK law (e.g. Curriculum and Assessment (Wales) Act 2021):

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Article 6(1)(e) of the UK GDPR)

If not, the school should consider each of the other lawful bases for processing in turn to assess how they fit with the processing and relationship with the data subject. As a public authority, please remember that legitimate interests cannot be used as a lawful basis when processing personal data to perform an official task or a public function.

The rules around consent should be considered carefully, as another lawful basis may be more appropriate. UK GDPR sets a high standard for consent and should put individuals in charge. Consent is now 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 consent must be freely given, specific, informed, and an unambiguous indication of wishes by a statement or affirmative action. As a result, consent forms should be clear and concise; include an opt-in, granular approach; as well as explain why information is collected and how it will be processed to inform individuals. Implied consent is no longer suitable.

The DPA2018 modifies the UK GDPR so that the minimum age for consent to be obtained from a child is lowered to 13 years old.

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."

The school should only use consent if none of the other lawful bases are appropriate. If you do so, you must be able to cope with people saying no (and changing their minds). Therefore, it's important that you only use consent for optional extras, rather than for core information the school requires to carry out its function. The below are examples where consent may or may not be appropriate;

- consent should be obtained when publishing a child's photo in any way (i.e. a school website, newsletter, prospectus, or social media).

- the school is required to hold learner and parent/carer details in a Management Information System (MIS). Therefore, it would not be appropriate to rely on consent, as the individual(s) would then have the right to opt out of the processing. In this case, the school could apply the public task lawful basis.
- The school is required to share information for the purposes of child protection issues. As a result, it would not be appropriate to rely on consent, as the individual(s) would have the right to opt out of the processing. The school could also alert an individual about an allegation made against them. In this case, the school could apply the public task lawful basis.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected and processed by a data controller:

- the identity and contact details of the data controller
- what categories of personal data are being processed
- the purposes and lawful basis for processing the personal data
- where and how the personal data was sourced
- to whom the personal data may be shared with
- whether any personal data is transferred to a country outside of the UK and EEA
- how long the personal data will be stored and retained
- the contact details of the Data Protection Officer
- the existence of automated decision making, including profiling
- data subject's rights and how to exercise them
- details of how to make a complaint to the school or ICO

The right to be informed is closely linked to the fair processing and transparency requirements of data protection principles. To comply, the school must provide parents/carers and learners with the above information when collecting personal data from individuals and ensure a privacy notice is easily accessible throughout the processing. For example, privacy notices could be passed to parents/carers and learners in the school prospectus, newsletters, or a specific letter/communication. The school could publish privacy notices on the school website. Parents/carers and learners who are new to the school should be provided with the privacy notice through an appropriate mechanism. Please be aware, however, that different forms of processing require a Privacy Notice, such as when processing visitor information or using personal data for employment purposes.

A school should ensure that privacy notices are available for learners as data subjects. Children and young people have the same rights as adults when it comes to their personal data. These include the rights described below and policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have several rights in connection with their personal data, which include:

- Right to be informed how personal data is collected, stored, managed, protected, and processed.
- Right of access to request a copy of personal information held of yourself. However, please be aware that information can sometimes be legitimately withheld.
- Right to rectification of inaccurate or incomplete personal data.
- Right to erasure where you have the right to have your personal data erased in certain circumstances. This does not include any personal data that must be retained by law.
- Right to restriction, which allows you to limit the way we use your personal data in some circumstances.
- Right to portability gives an individual the right to receive copies of data provided to a controller in a portable format.
- Right to object to the processing of one's personal data.
- Rights in relation to automated decision making and profiling.

Several of these are likely to impact schools, such as the right of access. Therefore, the school should put procedures in place to deal with Subject Access Requests and other individual rights requests (e.g. erasure and rectification).

Subject Access Requests are probably the most common individual right request made to any organisation. These are written or verbal requests to access all or a part of the personal data held by the Data Controller in connection with a living individual. Controllers have one calendar month to provide the information, unless the case is unusually complex and an extension can be obtained.

A school must consider all information requested for disclosure. However, there are instances where personal data must not be disclosed to the applicant, even if requested:

- the personal data of any third parties (not relating to the data subject)
- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- Individual Development Plans (IDPs) for learners with Additional Learning Needs (ALN)

Your school must provide the information free of charge. However, there are occasional instances where a reasonable fee can be charged, for example if the request is clearly unfounded, or excessive.

Personal data breaches and how to manage them

Schools are "data rich" and hold a large volume of personal data on the learners in their care. This data can be in paper (i.e. manual records) and electronic format (e.g. shared drives, electronic

databases, and Cloud solutions). Personal data is increasingly being held digitally with the introduction of electronic storage solutions (e.g. Google Drive) and the digital transfer or sharing of information. As a result, personal data is more accessible and the potential for data loss has increased significantly, especially where staff are working from remote locations (such as at home, other schools, or even public spaces).

Data protection law applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, this document will place emphasis on data that is held or transferred digitally due to being part of an overall Online Safety Policy template.

A personal data breach is described as a *"breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. As a result, there is more to a personal data breach than simply losing personal data, and breaches can be the result of both accidental and deliberate causes. For example, 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 or a learner, accidental loss of equipment or paper records, or equipment failure.

An important part of managing a personal data breach is for the school to have a clear and well understood procedure for reporting breaches so they can implement actions and minimise any further risk. The school should have a policy in line with the UK GDPR for reporting, logging, managing and recovering from incidents, which establishes:

- a "responsible person" for reporting and investigating incidents
- how to manage personal data breaches, including an escalation procedure
- criteria for determining incident level and timescales, which should help to:

The school may find it useful to develop an incident report form template for staff to complete if a personal data breach is discovered. These forms support the school to record all the information required to analyse the incident and comply with the accessibility principle. An example form should include the following.

All 'high risk' breaches must be reported to the Information Commissioner's Office through the DPO based upon the school procedure for reporting incidents. Data protection laws require this notification to take place within 72 hours of becoming aware of the breach (where feasible).

Schools must consider whether an incident discovered poses a risk to the individuals (i.e. data subjects) involved, including the likelihood and severity of any risk to people's rights and freedoms. If the assessment suggested a high risk is unlikely, the incident does not need to be reported. However, there is a legal duty under data protection law to document the facts relating to a breach,

its effects, and the remedial action taken by the organisation. The school should, therefore, maintain a log of all incidents.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) identify and assess privacy risks early on in a project that processes personal data to enable the school to mitigate them before the project launches.

DPIAs should be carried out by project leads under the support and guidance of the DPO. Schools should conduct a DPIA before processing activity starts and run alongside the planning and development process.

- Step 1: Identify the need for using personal data
- Step 2: Describe the information flows
- Step 3: Identify the privacy and related risks
- Step 4: Identify privacy solutions
- Step 5: Sign off and record the DPIA outcomes
- Step 6: Integrate the DPIA outcomes back into the project plan

Data protection law requires a DPIA to be completed where processing is likely to result in a high risk to the rights and freedoms of individuals and for the below types of processing:

1. Systematic and extensive profiling with significant effects
2. Large scale use of sensitive data (e.g. personal data, special category, or criminal data)
3. Public monitoring (i.e. CCTV)

For more information about DPIAs, please see this guidance on the ICO website.

A DPIA should contain the following:

- a description of the processing 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.

And could be laid out in this way:

Describe source of risk and potential impact on individuals	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant, or severe	**Overall risk** Low medium high*	**If medium or high, options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced, or accepted	**Residual risk** Low medium high*	**Measure approved** yes/no

A 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 those processing personal data will be assigned appropriate access. For example, 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, numbers, and special characters. User passwords must never be shared. Staff must also use multi-factor authentication (MFA).

Personal data may only be accessed on devices 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. personally 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 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 if applicable.

Clear policies and procedures should be in place for the use of "Cloud Based Storage Systems" (e.g. Microsoft 365, Google Workspace for Education). Please be aware that data held in remote and cloud storage is still required to be protected in line with the data protection laws. The school must ensure that it is satisfied with controls put in place by remote/cloud-based data services providers to protect the data. In Wales, all schools have access to Microsoft Office 365 and Google Workspace for Education via Hwb. For more information please visit .

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party. These require a Data Processor that is processing personal data on behalf of the school to:

- only act on the written instructions of the school
- ensure that staff processing the personal data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- only engage sub-processors with the prior consent of the controller, and under a written contract
- assist the controller in providing subject access to information and allowing data subjects to exercise their rights under the UK GDPR
- assist the controller in meeting its data protection obligations in relation to the security of processing, including the notification of personal data breaches and carrying out DPIAs
- delete or return all personal data to the controller as requested at the end of the contract
- provide the controller with whatever information it needs to ensure that they are both meeting their data protection obligations
- tell the controller immediately if it is asked to do something infringing the UK GDPR, Data Protection Act 2018

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/restricted/protected personal data from the school or authorised premises without permission. Media should be encrypted and password protected and transferred 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.
- Secure remote access to a management information system or learning platform is preferable when personal data (particularly special categories of personal data) is required by an authorised user from outside the organisation's premises (e.g. by a member of staff to work from their home). 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 transferred to another country (particularly outside the UK and EEA) and advice should be sought from the Data Protection Officer in this event.

Disposal of personal data

The school should implement a retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society's 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 record of destruction log (i.e. Schedule for Disposal/Destruction) should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records 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 (DPO)
- 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 personal 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.

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, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the personal data

Data Protection Fee

Schools are required to pay the relevant annual fee to the Information Commissioner's Office (ICO) by law. This means the school is breaking the law if, as a data controller, it processes personal data and have either not paid a fee, or not paid the correct fee.

Responsibilities

Every school is required to appoint an independent Data Protection Officer (DPO) 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 DPIA
- 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 law.

The school may also wish to appoint a Data Manager or Information Governance Lead. 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 information risk policy and risk assessment
- oversee the System Controllers.

The school may also wish to appoint staff members to be responsible for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These staff members 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 (including learner data) in a safe and secure manner.

The school may wish to consider appointing a designated governor for data protection, however, all governors are required to comply fully with this policy where they have access to personal data as part of their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff and governors must receive data handling awareness and 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
- Annual data protection training for all staff
- Staff meetings / briefings / INSET
- Day to day support and guidance

The school curriculum should ensure that children and young people understand their rights and privacy implications. Advice and guidance are available from the ICO and Hwb.

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase "openness by design" in public sector organisations as part of a healthy democratic process. FOI requests are submitted by an individual and the school are required to consider whether the requested information should be released into the public domain. Any requests for personal data should be dealt with under data protection law. The FOI Section 40(1) and (2) exemption covers 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 policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, and coordinate FOI (including related policies and procedures). The school should 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 publication scheme should be reviewed annually.

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

Parental permission for use of cloud hosted services

Schools that use cloud hosting services are advised to identify the relevant lawful basis 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 that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in 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 law.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

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

Privacy and Electronic Communications

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

C3 Device Management Policy Template (including Bring Your Own Device)

Suggestions for use

Within this template sections which include information or guidance are shown in BLUE. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in italics it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL Online Safety Group that these would be an essential part of a school Online Safety Policy.

Devices may be a school owned/provided or privately owned smartphone, tablet, laptop or other technology that usually has the capability of utilising the school wireless network. The device then has access to the wider internet which may include the school's virtual earlning platform and other cloud-based services such as email and data storage.

The key to considering the use of devices is that the learners, staff and wider school community understand that the primary purpose of having a device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The device management policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of technology should be included in the digital competence and online safety education programme.

Potential Benefits of Devices

Research has highlighted the widespread uptake of devices amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital resilience, fluency and citizenship in learners that will prepare them for the technology-driven world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing devices. These 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.

Schools may consider implementing the use of Bring Your Own Devices (BYOD) as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of devices brings both real benefits and challenges for the whole school community – including practitioners - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of device implementations is possible. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of devices
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[7]	Learner owned	Staff owned	Visitor owned
Allowed in the school	Yes	Yes	Yes	Yes/No[8]	Yes/No[8]	Yes/No[8]
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						

[7] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[8] The school should add below any specific requirements about the use of personal devices in the school e.g. storing in a secure location, use during the day, liability, taking images etc..

No network access						

The school has provided technical solutions for the safe use of school devices/personal devices (delete/amend as appropriate):

The school has provided technical solutions for the safe use of school devices/personal devices (delete/amend as appropriate):

- All school devices are controlled though the use of a Mobile Device Management (MDM) solution.
- Appropriate access control is applied to all devices according to the requirements of the user.
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all devices, filtering will be applied to the internet traffic and attempts to bypass this are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include: revoking the link between MDM solution and the device; removing proxy settings; ensuring no sensitive data is retained on the device; uninstalling school-licenced software etc..
- *All school devices are subject to routine and pro-active monitoring.*

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passwords, PINs or alternative security controls (i.e. biometrics) should be set on personal devices to aid security.

- The school is not responsible for the day-to-day maintenance or upkeep of personal devices such as the charging, the installation of software updates or the resolution of hardware issues.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:
    - Devices may not be used in tests or exams.
    - Visitors should be provided with information about how and when they are permitted to use devices in line with local safeguarding arrangements.
    - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of infecting the network.
    - Users are responsible for charging their own devices and for protecting and looking after their devices whilst in the school.
    - Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day.
    - Devices must be in silent mode on the school site and on school buses.
- School devices are provided to support learning. It is expected that learners will bring devices to the school as required.
- The changing of settings (exceptions include personal and accessibility settings by the user that would stop the device working as it was originally set up and intended to work is not permitted.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- The school will ensure that devices contain the necessary apps for schoolwork. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases they use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.
- Printing from personal devices will not be possible.

Insurance

Schools that have implemented an authorised device approach (1:1 deployment) may wish to consider how they will insure these devices and should include details of the claims process in this policy.

C4 Social Media Policy Template

Social media (e.g. Facebook, X (formerly 'Twitter'), LinkedIn, Instagram) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which social media can offer. Staff, parents and carers and learners are actively encouraged to find creative ways to engage with social media. However, there are some risks associated with social media use, particularly regarding the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and learners.

Scope

This policy is subject to the school codes of conduct and acceptable use agreements.

This policy:

- applies to all staff and to all online communications which directly or indirectly, represent the school
- applies to such online communications posted at any time and from any platform
- encourages the safe and responsible use of social media through training and education
- *defines the monitoring of social media activity pertaining to the school.*

The school respects privacy and understands that staff and learners may use social media in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.
Personal communications are those made via 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.

Digital communications with learners are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- *The Senior Leadership Team (SLT) are responsible for*
    - Adhering to Welsh Government Practices and principles for schools' use of social media.
    - Facilitating training and providing guidelines on Social Media use (see Welsh Government social media guidance).
    - Agreeing social media account monitoring requirements.
    - Developing and implementing the school's Social Media policy.
    - Consideration and approval of account creation.
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

- *Administrators/moderators are responsible for*
    - Creating the social media accounts following SLT approval.
    - Storing account details, including passwords securely.
    - Undertaking the monitoring and oversight of accounts.
    - Ensuring that all access to accounts is controlled (i.e. in the event of staff turnover or changes to roles and responsibilities).

- *Staff are responsible for*
    - Knowing the contents of and ensuring that any use of social media is carried out in line with this and other relevant policies.
    - Attending appropriate training.
    - Regularly monitoring, updating and managing content they have posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school.

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points: **Anyone wishing to create such an account will consider the questions below as part of any decision-making before an account is created.**

- What is the aim of the account?
- Who is the intended audience?
- How will the account be promoted?
- Who will manage the account? (It is recommended that at least 2 staff members manage any account, and notwithstanding this, schools should identify a responsible owner for each account, who may be a member of the senior leadership team)
- How will the account be monitored?
- How will the account be configured: open, private or closed?
- Are staff clear as to how and for what purpose each communication method will be selected?
- From where will the account be accessed?
- What are the escalation procedures should something go wrong?

In all cases, the SLT will ensure that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents and carers.

Monitoring

School accounts are monitored regularly and frequently. The school checks for inappropriate or unauthorised content and promptly responds to and addresses any issues. School accounts may not be monitored or responded to outside of school hours or school holidays. During periods where the account is not monitored, the school may 'pin' appropriate messages to the profile advising when a response should be expected. These are prominent fixed messages and often appear at the top of a social media feed.

Monitoring posts about the school

- As part of active social media engagement, the school will pro-actively monitor the internet for public postings about the school.
- The school will respond to social media comments made by others according to a defined policy or process.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media, staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely serious by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, will seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Managing incidents

The school recognises that abusive and harmful behaviours carried out through social media may impact staff and learners, and the schools' reputation.

- If an individual is subject to abuse through the use of social media channels associated with the school, then this action will be reported using the agreed school protocols and appropriate access to support will be made available.
- When acting on behalf of the school, offensive comments will be handled swiftly and with sensitivity.
- It may be necessary to block individuals from interacting with the school's social media channel if they do not adhere to the acceptable use agreement. Grounds for blocking may include harassment, offensive language, inappropriate content, spamming and any other behaviour that goes against the school's values or principles as set out in the expectations for use.
- If a user is blocked they will be informed exactly why the action was taken

Use of images

School use of images can be assumed to be acceptable, providing permission to use any photos or video recordings is sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes will be respected.

Staff must strictly adhere to the following guidelines:

- Under no circumstances should staff share or upload learner pictures online other than via school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use of social media accounts

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

- *Learners*
  - Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media network account.
  - The school has a cross-curricular approach to educate learners to be safe and responsible users of social media.
  - Any offensive or inappropriate comments relating to the school will be resolved by the use of the school's behaviour policy

- *Parents and Carers*

- If parents and carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- In the event of any offensive or inappropriate comments being made about the school, the school will ask the parent or carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

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 event 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.

Schools may wish to view the National Crime Agency (NCA) website which includes information about "Cyber Choices: Helping you choose the right and legal path". The TARIAN Regional Cyber Crime Unit (RCCU) now has dedicated 'Cyber Prevent' officers whose role is to prevent young people from committing cybercrime and/or re-offending. Supportive resources are available on Hwb and there is a useful summary of the Computer Misuse Act on the NCA site.

The Data Protection Act 2018:

DPA2018 updates the 1998 Act, and incorporates the UK General Data Protection Regulation (GDPR) and aims to:

- facilitate the secure transfer of information in the UK and within the European Economic Area (EEA)
- prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives and organisation
- give the public confidence about how organisations can use their personal information
- provide data subjects with the legal right to check the information organisations hold about them. They can also request for the data controller to destroy it
- give data subjects greater control over how data controllers handle their data
- place emphasis on accountability. This requires organisations to have processes in place that demonstrate how they're securely handling data
- require organisations to keep people's personal data safe and secure. Data controllers must ensure that it is not misused
- require the data user or holder to register with the Information Commissioner's Office (ICO).

All data subjects have the right to:

- receive clear information about what you will use their data for
- access their own personal information
- request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan
- prevent or query about the automated processing of their personal data.

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 must follow a number of set procedures and deadlines.

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, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, 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 to:
    - ascertain whether the communication is business or personal
    - protect or support help line staff
- the school reserves the right to monitor its systems and communications in line with its rights under this act.

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. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

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

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 Harassment 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 anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

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. Children, Families and Education Directorate page 38 April 2007.

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.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Protection of Freedoms Act 2012

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

Serious Crime Act 2015

This Act introduced a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an adult individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison. For further guidance or support please contact the Revenge Porn Helpline

Online Safety Act 2023

The Online Safety Act enhances the safety of users on the internet, particularly focusing on the protection of children and vulnerable individuals from harmful online content. The Online Safety Act defines 'priority offences' including

- child sexual abuse and grooming;
- encouraging or assisting suicide or serious self-harm;
- harassment, stalking, threats and abuse;
- controlling or coercive behaviour;
- intimate image abuse;
- sexual exploitation of adults

It focusses on online services which host content posted by other people ("user-to-user services" such as Facebook, Instagram and Twitter) and search services (such as Google, Yahoo and Bing). The Bill has different levels of protection for children and adults.

Protections for young people

The Online Safety Act creates a legal responsibility (a "duty of care") for the operators of user-to-user services to protect users under the age of 18 from harmful content, specifically

- Enforcing minimum age requirements
- Publishing risk assessments
- Protecting children from harmful content published on the service
- Properly applying the Terms and Conditions

Protections for adults

While the Bill focusses on the need to protect young people online, there are some provisions that focus on protecting adults (which will benefit all users) including

- Ability to customise your feed
- Block online trolls
- Criminalising certain content
- Remove content that is already illegal

Enforcement

Ofcom has been appointed as the regulator and have powers to obtain information from website operators on how they deal with online harms and to take action if they fail to comply with their new duties, including

- Investigate website operators and their compliance with the Bill
- Issue financial penalties to companies that do not comply with their obligations
- Issue guidance on compliance
- Issue notices requiring website operators to give information or cooperate with an Ofcom investigation

Domestic Abuse Act 2021

Section 69 of the Domestic Abuse Act 2021 establishes the legal offence related to the threat of revealing private sexual images or videos featuring another person. This offence occurs when someone threatens to share such content with the intent to distress the individual depicted, and the sharing would happen without that individual's consent.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school Online Safety Policy and creating their online safety provision:

Welsh Government

Safeguarding children (including Keeping Learners Safe and Respect and resilience: developing community cohesion)
School bullying advice

Hwb

Hwb homepage
Keeping safe online
Hwb Support Centre
Hwb Trust Centre
Education Digital Standards
Enhancing digital resilience in education: An action plan to protect children and young people online - 2020
Online safety: Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners
Digital Competence Framework
Health and Well-being AOLE
Keeping Learners Safe Modules 4 and 5 Online Safety for Practitioners and Governors
Live-streaming and video-conferencing: safeguarding principles and practice
Safer Internet Day resources
Hwb resources for governors
Advice for schools on preparing for and responding to viral online harmful challenges and hoaxes
Practices and principles for schools' use of social media

UK Safer Internet Centre

UK Safer Internet Centre
South West Grid for Learning
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation
Report Harmful Content
UK Safer Internet Centre – Research Summaries

Others

CEOP

CEOP Education

INSAFE/Better Internet for Kids

UK Council for Internet Safety (UKCIS)

Tools for Schools

SWGfL Test filtering

UKCIS Digital Resilience Framework

SWGfL Swiggle Child Friendly Searching

Bullying/Online-bullying/Sexting/Sexual Harassment

Childnet – Project deSHAME – Online Sexual Harassment

Hwb A teacher's guide to recognising and challenging online bullying

Estyn - We don't tell our teachers - Experiences of peer-on-peer sexual harassment among secondary school pupils in Wales

Data Protection

ICO Support for organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

ICO – Education Data

NCSC – Education and Skills - Schools

Infrastructure/Technical Support

UKSIC Appropriate Filtering and Monitoring

Hwb Recommended filtering standards for schools in Wales

NCA Guide to the Computer Misuse Act

NEN Advice and Guidance Notes

Working with parents and carers

Childnet Webpages for Parents & Carers

Get Safe Online resources for parents

Internet Matters

Hwb App guides for families

Prevent

Prevent Duty Guidance

NCA CyberChoices

TARIAN Regional Cyber Crime Unit (RCCU)

Hwb TrustMe

Hwb A teacher's guide understanding the role of the internet in extremism and radicalisation

Research

Ofcom –Media Literacy Research

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use. Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in March 2024. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2024