Online Safety Policy

This document was: Generated by the Headteacher/ Senior Management Team/ Staff October 2021

Reviewed/revised at a meeting of the full Governing Body held on 17th November 2021;

Reviewed/ Revised/ Approved at a meeting of the full Governing Body held on 22nd March 2023; 21st June 2023

Review date: June 2025

Signed: _____ Chairperson schools governing body, on behalf of the governing body

Date: _____

Signed: _____ Headteacher

Distribution: Staff, governors, pupils, parents/carers and the wider community as requested

Acknowledgements

The governing body of Ysgol Ty Coch Special School having fully considered the content of the Online Safety Policy has resolved to accept it as a working document.

The content of the policy and Appendix to be applied across the school as appropriate.

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Ysgol Ty Coch Special School to safeguard members of our school community online in accordance with statutory guidance and best practice. 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 digital technology on the school site (where allowed).

The school 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 , Online Safety Group made up of:

- *headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/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:*	*22nd March 2023*
The implementation of this Online Safety Policy will be monitored by:	*Ashlie Holland*
Monitoring will take place at regular intervals:	*Annually*
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:	*Annually*
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:	*June 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA safeguarding officer, police etc*

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:*
    - o *learners*
    - o *parents and carers*

Policy and leadership

Responsibilities

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 the Online Safety Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant 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

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy This review will be carried out by governors 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 to include:

- **regular meetings with the Online Safety Lead**

---

[1]

[2]

- **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
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), 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 / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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[3] 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/MAT/external provider) 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/MAT/relevant body.

---

[3]

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data [4]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

Curriculum/AoLE Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through:
- a discrete programme
- context booklets
- PHSE and RSE programmes
- developing a mapped cross-curricular programme
- 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)
- they immediately report any suspected misuse or problem to designated safeguarding officer/ online safety officer for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- 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

---

[4]

- 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 regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- 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/MAT/technology provider) is responsible for ensuring that:
- they are aware of and follow the school Online Safety Policy and Technical Security Policy 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/MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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 technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to SLT for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person monitoring software/systems are implemented and regularly updated as agreed in school policies

Learners
- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- 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 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

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

Online Safety Group

The Online Safety Group has the following members;

- Online Safety Lead - Ashlie Holland
- Designated Safeguarding Lead – Headteacher David Jenkins until 31.08.23 and Simon Wilson from 01.09.23
- senior leaders - SLT
- online safety governor - Janice Stuckey and Lyndon Walker
- technical staff - Extrascope
- teacher and support staff members - Chris Myhill/Tanya Evans Debbie Ramsay, Jonathan Woodrow
- learners - digital champions
- parents/carers
- community representatives

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible

- encouraging the contribution of learners to staff awareness, emerging 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 self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., 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 should use digital technologies responsibly, protecting themselves and the school and how they should 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
- 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

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online 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:	**Any illegal activity for example:** ● 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 images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 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 – further information here					X
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	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list. ==Ashlie download and add x then upload==	Staff and other adults				Learners			
	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 e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

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

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school**
- **any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.** Personal e-mail addresses 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 e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

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.**
- **all members of the school community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm** (see flowchart and user actions chart in the appendix), **the incident must be escalated through the agreed school safeguarding procedures.**
- any concern about staff misuse will be reported 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 / MAT
- where 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 device 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 device for the duration of the procedure.
- ensure that the relevant staff 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
- 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:
  - o internal response or discipline procedures
  - o involvement by local authority / MAT (as relevant)
  - o 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 reporting or affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
  - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - key staff, involved with the incident
  - Safeguarding team /My Concern

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 Flowchart

Unsuitable materials or activity

↓

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

↓

If staff/volunteer or learner, 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 required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

↓

Implement changes → Monitor situation

The DSL/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.

Illegal materials or activities found or suspected

↓

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

↓

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

↓

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

↓

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.

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:

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 rights	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	X		X	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	X						
Corrupting or destroying the data of other users.	X	X	X					X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X			X			
Using proxy sites or other means to subvert the school's filtering system.	X	X	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X				X	X			

Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X		X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X								
Unauthorised use of digital devices (including taking images)	X								
Unauthorised use of online services	X								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X			X		X	
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			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	X	X		X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X		X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X		X		X	X
Unauthorised downloading or uploading of files or file sharing	X	X				X		
Breaching copyright or licensing regulations.	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	x	x				X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x		
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	x	x				x		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	x	x						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x	x	x		x	x	x	x
Actions which could compromise the staff member's professional standing	x	x				x		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	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				x		

Online Safety Education Programme

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

- **A planned online safety curriculum for all year groups.**
- **Lessons are matched to need; are age-related and build on prior learning**
- **Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes and highlighted in schools context booklets.**
- **Learner need and progress are addressed through effective planning and assessment**
- **Digital competency is planned and effectively threaded through the appropriate digital pillars and throughout all the areas of learning.**
- **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.**
- 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 should be able to request the temporary removal of 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 should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

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
- 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
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **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 Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / 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 several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents

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

Families

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,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).

Technology

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

Filtering

- 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/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed 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
- there is a clear process in place to deal with requests for filtering changes

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

Monitoring

The school has monitoring systems in place to protect the school, systems and users:
- **The school monitors all network use across all its devices and services.**
- **An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.**
- **There are effective protocols in place to report abuse/misuse. 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

- **Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.**

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment.

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- **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**
- **all users (adults 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. Users must immediately report any suspicion or evidence that there has been a breach of security**
- **all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password** by Ashlie Holland 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.**
- **passwords should be long.**
- records of learner usernames and passwords for learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Ashlie Holland/Extrascope is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.

- 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 and devices 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 endpoint (anti-virus) software.
- 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 systems
- an agreed policy is in place, AUP provided by WG 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
  -downloading executable files and installing programmes on school devices
  -the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
  preventing the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

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

The school allows:

	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**	No	Yes	Yes/No
Allowed in college	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	no	no	no	no	no	no
Internet only	YES	Yes	Yes	yes	Yes	yes

School owned/provided devices:

Use of mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, learners and staff to follow the rules set out in the AUP

Personal devices

Use of mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, learners and staff to follow the rules set out in the AUP

Social media

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
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

---

[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.

- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:
- 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 personal social media sites during school break and lunch times

Monitoring of public social media
- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process which will be assessed according to the circumstances.
- 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.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm;
- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.**
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**

- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes**
- 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
- care should be taken when sharing digital/video images that learners are appropriately dressed
- 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 Online Safety Policy
- **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.**
- **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 in line with the school retention policy**

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through;
- Public-facing website
- Social media
- Online newsletters
- Seesaw learning platform

The school website is managed/hosted by the school. The school ensures that online safety policy has been followed 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 least 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 and acceptable use agreements; 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 Protection

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

The school:
- **has a Data Protection Policy.**
- **implements the data protection principles and 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 effective understanding of data protection law and is free from any conflict of interest.**
- **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 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **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,**
- **carries out Data Protection Impact Assessments (DPIA) 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**

- **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.**
- **has clear and understood policies and routines for the deletion and disposal of data**
- **[reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents**
- **has a Freedom of Information Policy which sets out how it will deal with FOI requests**
- **provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff**

When personal data is stored on any mobile device or removable media the:
- **data will be encrypted, and password protected.**
- **device will be password protected.**
- **device will be protected by up-to-date endpoint (anti-virus) 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:
- **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 data storage for personal data**
- **will not transfer any school personal data to personal devices. Staff will be provided with school owned devices and follow the AUP in relation to home working/access.**
- **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.**

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 found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the SWGfL website. The appendices are as follows:

A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template

A9 - Responding to incidents of misuse – flow chart

A10 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A11 - Reporting Log

B1 - Training Needs Audit Log

C1 - Technical Security Policy Template (including filtering and passwords)

C2 - Personal Data Advice and Guidance

C3 - School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)

C4 - Mobile Technologies Policy Template (inc. BYOD/BYOT)

C5 - Social Media Policy Template

Legislation
Links to other organisations and resources
Glossary of Terms

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 online safety self-review tool:

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

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

School Online Safety Policy Template Appendices

Appendices

A1 - Learner Acceptable Use Agreement Template – for older learners

A2 - Learner Acceptable Use Agreement Template – KS2

A3 - Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)
A4 - Parent/Carer Acceptable Use Agreement Template
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A6 - Community Users Acceptable Use Agreement Template
A7 – Online Safety Group Terms of Reference Template

A8 - Harmful Sexual Behaviour Policy Template (new template added September 2022)

A9 - Responding to incidents of misuse – flow chart

A10 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A11 - Reporting Log

B1 - Training Needs Audit Log

C1 - Technical Security Policy Template (including filtering and passwords)

C2 - Personal Data Advice and Guidance

C3 - School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)

C4 - Mobile Technologies Policy Template (inc. BYOD/BYOT)

C5 - Social Media Policy Template

Legislation

Links to other organisations and resources

Glossary of Terms

A5 Staff, Volunteer and Community Acceptable Use Policy Agreement Template

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 for learning 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 young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the 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 school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school 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 school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line 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 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.
- I will not use personal email addresses on the school's ICT systems.

- 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.
- 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 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 online systems 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's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include) a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

General Data Protection Regulation (GDPR)

I understand that GDPR relates to data which is not solely electronic in nature. I confirm that I have read and understand my responsibilities in relation to GDPR which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes

- Adequate, relevant and not excessive

- Accurate

- Kept no longer than is necessary

- Processed in accordance with the data subject's rights

- Secure

- Only transferred to others with adequate protection.

Staff must ensure that they:

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

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.

- Safeguard Paper records which should be stored in locked cupboards

- Reduce the amount of time paper records are taken off site. Where this is unavoidable, suitable controls should be in place e.g. locked suitcases, not left in cars etc…

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

- School data must not be stored on personal devices

- The data must be encrypted and password protected

- The device must be password protected and supplied by schoolThe device must offer approved virus and malware checking software

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

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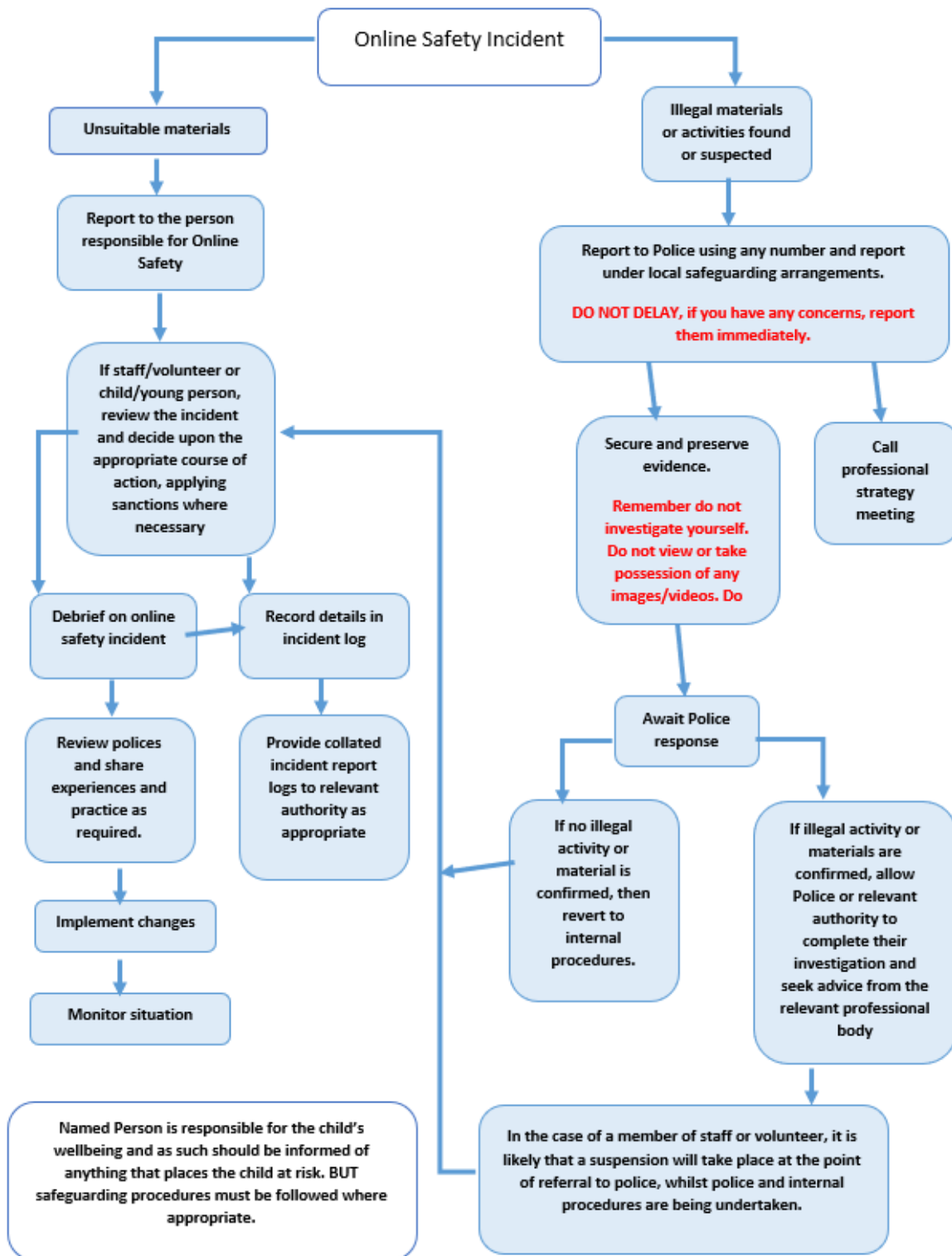
Staff/Volunteer Name: _____

Signed: _____

Date:

A9 Responding to incidents of misuse – flow chart

Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

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

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

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.

A10 Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

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

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A11 Reporting Log

Group: _____

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

B1 Training Needs Audit Log

Group: _____

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

Policy informed by;

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 website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:
- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses 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 businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms 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.

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 to follow a number of set procedures.

Communications Act 2003

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

Malicious Communications Act 1988

It is an offence to send an indecent, 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, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;

- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- 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 Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -
http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced 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 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

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:

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour -
http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_H
eadteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA   Acceptable Use Policy/Agreement – see templates earlier in this document

CEOP   Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPD   Continuous Professional Development

FOSI   Family Online Safety Institute

ICO   Information Commissioners Office

ICT   Information and Communications Technology

INSET   In Service Education and Training

IP address   The label that identifies each computer to other computers using the IP (internet protocol)

ISP   Internet Service Provider

ISPA   Internet Service Providers' Association

IWF   Internet Watch Foundation

LA   Local Authority

LAN   Local Area Network

MAT   Multi Academy Trust

MIS   Management Information System

NEN   National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom   Office of Communications (Independent communications sector regulator)

SWGfL   South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK   Think U Know – educational online safety programmes for schools, young people and parents.

UKSIC   UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

UKCIS   UK Council for Internet Safety

VLE   Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP   Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Equal Opportunities

The school operates a policy of equality for all pupils regardless of gender, ethnicity, religious beliefs or culture.

All staff at Ysgol Ty Coch Special School take account of each pupil's learning styles/needs and their development and wellbeing; and how these are affected by a range of social, religious, ethnic, gender, cultural and linguistic differences.

Pupils identified as Children Looked After (CLA), More Able and Talented (MAT) and those on the child protection register are supported in line with their particular needs to afford them equal access to the curriculum.

Safeguarding

The Safeguarding of pupils is of paramount importance. The school understands its duty to keep learners safe and adheres to the PREVENT agenda and broader safeguarding guidelines. Regular and well planned lessons are taught in online safety.

Staff Development

Staff will have access to in-service training as and when appropriate. This is in accordance with the school's policy for staff development. Any new developments in Online Safety will be disseminated by the ICT PLC throughout the year.

Role of the Head teacher

• 	To discuss future developments for Online Safety with the ICT PLC

• 	 Facilitate training and guidance on Social Media use.

• 	 Develop and implementing the Social Media policy

• 	Take a lead role in investigating any reported incidents.

• 	Make an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

- Receive completed applications for Social Media accounts

- Approve account creation

- Ensure budget provision for current resources and materials

- Ensure budget provision for staff training

Links to Other Policies

- Safeguarding

- Management of Health and Safety at Work

- Password Management

- Physical Security

- Preventing Extremism

- Disciplinary Procedure for School Based staff

- Internet and Email Acceptable Usage

- Mobile Phone

- Anti bullying

Appendix

Ysgol Ty Coch Distance learning policy

Adapted from: Safeguarding Considerations for Distance Learning v3 3.6.20

The following document has been revised following publication of further advice by the Welsh Government. The most relevant current documents are linked below.

Approaches to support distance learning

In extenuating circumstances distance learning may apply for some learners.
School staff should discuss with the Designated Safeguarding Lead any issues or concerns prior to using technology to support teaching and learning or any issues as they arise during use.

Acceptable use

The acceptable use policy that is used for the use of technology in school should be applied when using technology for distance learning for both staff and pupils. The Hwb also provides a 360 degree Safe Cymru tool to support the school's online safety policy and practice available at the following link:

https://hwb.gov.wales/zones/online-safety/repository/resource/6f3b56cd-439c-49a9-bc64-696223b85466/en

Platforms

Direct communication with students/parents should be carried out using SeeSaw, school Google email, RCT corporate emails and other approved platforms/devises such as class Hwb, TEAMS and mobile phones. Video calls to people outside the school Google Network should be undertaken on TEAMS via Hwb e.g. Parents Evening

Careful consideration should be given to the privacy notice and the level of control and security in place to safeguard all involved. School provided accounts should be used by pupils and school provided devices used by staff.

Considerations

Accountability

Decision-making at a school level may determine whether live streaming is appropriate to host lessons with learners. As in any school setting, all accountability is owned by the headteacher and governing body of the school. Headteachers and governing bodies must ensure that the Welsh Government guidance referenced in this document is observed alongside local authority guidance. Any live streaming should be done on a voluntary basis and staff should not be directed to undertake live streaming of lessons.

Professional Issues

Live streaming of lessons (**synchronous** teaching) is only permitted with the explicit permission of the Headteacher. Any education practitioners choosing to live stream should continue to work in the same professional manner as they would in the classroom. There should always be at least two members of teaching staff online and present at all times during any live-streamed lesson. One-to-one live-streaming lessons with learners should not be undertaken and consideration given to the fact that all comments will be heard by a number of learners and could be potentially misconstrued. Consideration should also be given to confidentiality when live streaming a lesson from a venue where other adults or children are present. The school does not permit recording of synchronous activities.

If lessons are recorded to be shared with learners at a later date, this should be done as an asynchronous activity without learners being present in the recording. Recordings must not be used for any teacher evaluation purposes.

Asynchronous

Asynchronous sessions give both learners and teachers flexibility and a safer environment to work in, minimising the unexpected whilst ensuring interaction. Pre-prepared video, podcasts and other content can be posted through the chosen learning platform and an outline provided to pupils as to how they can post responses.

Setting

If pupils are asked to record and submit any work via video, or take part in synchronous learning activities, clear advice should be provided about the setting. For pupils and staff it would be inappropriate for them to be in their bedroom for example. Pupils should be encouraged to be in a social space, preferably

accompanied by their parent or other adult and ensure that the background is free of inappropriate/personal items. Staff must also be alert to the pupil and their own setting and the possibility of others in the background displaying inappropriate behaviour/language and pupils seeing a member of staff's personal items. Many platforms allow staff to change their background setting and this should be used where available by staff and learners.

Network connection

Consideration should be given to the fragility of each pupil's network connection (or if they even have one). Children are likely to get stressed if their internet connection cannot effectively engage with the technology being used and could potentially fear of missing out in an educational environment. Homes with multiple learners and parents working from home may also mean a lack of equipment to use. Wi-Fi use should be encouraged to avoid potential network costs if learners choose to use mobile phone data.

Length of session

Sessions should be kept as short as possible and used to give a brief overview of the topics that need to be covered in a given time period. Tasks can be set, submitted and reviewed before the next session. At the end of any synchronous sessions, care should be taken to ensure all learners have left before staff leave. This way staff will ensure that they are not facilitating an environment where learners are alone and unsupervised in an online room which has been created by them.

Behaviour

Clarity should be provided about the expectations of both student and staff behaviour (e.g., a 'classroom standard' of behavior/appropriate clothing/language is expected from all participants).

'Live-streaming safeguarding principles and practice for education practitioners' (link above) contains an example agreement for use in live streaming activities that could be disseminated to learners/parents prior to using this approach.

This is something that I will look to produce an exemplar of and use with Post 16

Digitally Excluded Learners

Distance learning may not be possible for some digitally excluded learners. These need to be identified by schools and alternative models of distance learning explored. In the interest of equity, offline learning activities should be provided for all learners unable to access technology while the issue of their connectivity is being addressed

Appendix 5 - Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

1. I will only use ICT in school for school purposes

2. I will only open e-mail attachments from people I know, or who my teachers have approved

3. I will not tell other people my ICT Passwords

4. I will only open/delete my own files

5. I will make sure that all ICT contact with other children and adults is reasonable, polite and sensible

6. I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidently find anything like this, I will tell my teacher

7. I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me

8. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe

9. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community

10.   I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my online safety

11.   If I am unsure about anything, I will ask a member of Ysgol Ty Coch Special School staff for help

Signed (child):……………………………………………

Signed (parent): …………………………………………..

Appendix 4 :Ysgol Ty Coch Special School Online Safety Parent / Carer Code of Conduct

Code of Conduct

At Ysgol Ty Coch Special School we value the strong relationship with parents and carers. Together, this helps us achieve the very best for the children in a mutually supportive partnership between parents, class teachers and the school community.

As a partnership, parents understand the importance of a good working relationship with the school. We continually welcome and encourage parent and carers to participate in the life of the school. Parents and carers are always encouraged to contact the school with any concerns and/or issues. The school would appreciate the opportunity to resolve any matter with parents and carers.

Parents, carers and visitors are reminded:

- To respect the caring ethos and values of the school;

- That both teachers and parents need to work together for the benefit of their children;

- Approaching school staff for help to resolve an issue is done in an appropriate manner; and

- All members of the school community are treated with respect using appropriate language and behaviour.

The school will not tolerate:

- Disruptive behaviour which interferes or threatens to interfere with any of the schools operation or activities anywhere on the school premises;

- Any inappropriate behaviour on the school premises;

- Use of loud or offensive language or displaying temper;

- Threatening, in any way, a member of staff, visitor, fellow parent/carer or pupil;

- Damaging or destroying school property;

- Sending abusive or threatening e-mails or text/voicemail/phone messages or other written communications to anyone within the school community;

- Defamatory, offensive or derogatory comment regarding the school or any of the pupils/parents/staff at the school on Facebook or other social sites (see appendix 1)

Should any of the above occur on school premises, the school may feel it necessary to take action by contacting the appropriate authorities and / or consider banning the offender from entering the school premises.

'Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by providing information, signposting to services, sharing opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation, engagement, pass information and services over a wide network of people. This could include blogs, message boards, social networking websites (such as Facebook, Twitter, LinkedIn, My Space) and content sharing websites (such as Flickr, Youtube) and many other similar online channels.

Definitions of misuse or inappropriate behaviour

The following actions may constitute misuse of social media or inappropriate behaviour; it is however by no means exhaustive:

- · Publishing materials that might be considered inappropriate, offensive or libellous

- · Publishing materials considered to be defamatory or to the detriment of the School and its community

In the event that any pupil/parent/carer of the school is found to be posting libellous or defamatory comments on Facebook or other social media network sites, they will be reported to the appropriate "report abuse" section of the network site. The school will also expect the pupil/parent/carer to remove such comments immediately. The school will consider its legal options to deal with any such misuse or inappropriate behaviour.