Respect. Communicate. Enjoy.

Online Safety Policy

Reviewed or revised at a meeting of the Standards Committee on the:	13th November 2025
Reviewed/approved at a meeting of the full Governing Body held on:	20th November 2025
Next Review date:	November 2028

Signed Date

Chairperson schools governing body, on behalf of the Governing Body

Signed Date

Headteacher

Distribution: Staff, governors, pupils, parents/carers and interested parties.

Acknowledgements

This policy has been written seeking extensive advice from Welsh Government (WG) and South West Grid for Learning (SWGfl). We would like to acknowledge these organisations and 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 degree safe e-Safety Self Review Tool:

- Members of the SWGfL e-Safety Group
- Representatives of SW Local Authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

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:	**November 2025**
The implementation of this Online Safety Policy will be monitored by:	**SLT**
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:	**October 2026**
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:
    - learners
    - parents and carers

- staff.

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:

2

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

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

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- 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.

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
- PSE 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
- 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 Simon Wilson
- senior leaders - SLT
- online safety governor - Janice Stuckey
- technical staff - Extrascope
- teacher and support staff members
- 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	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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.	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

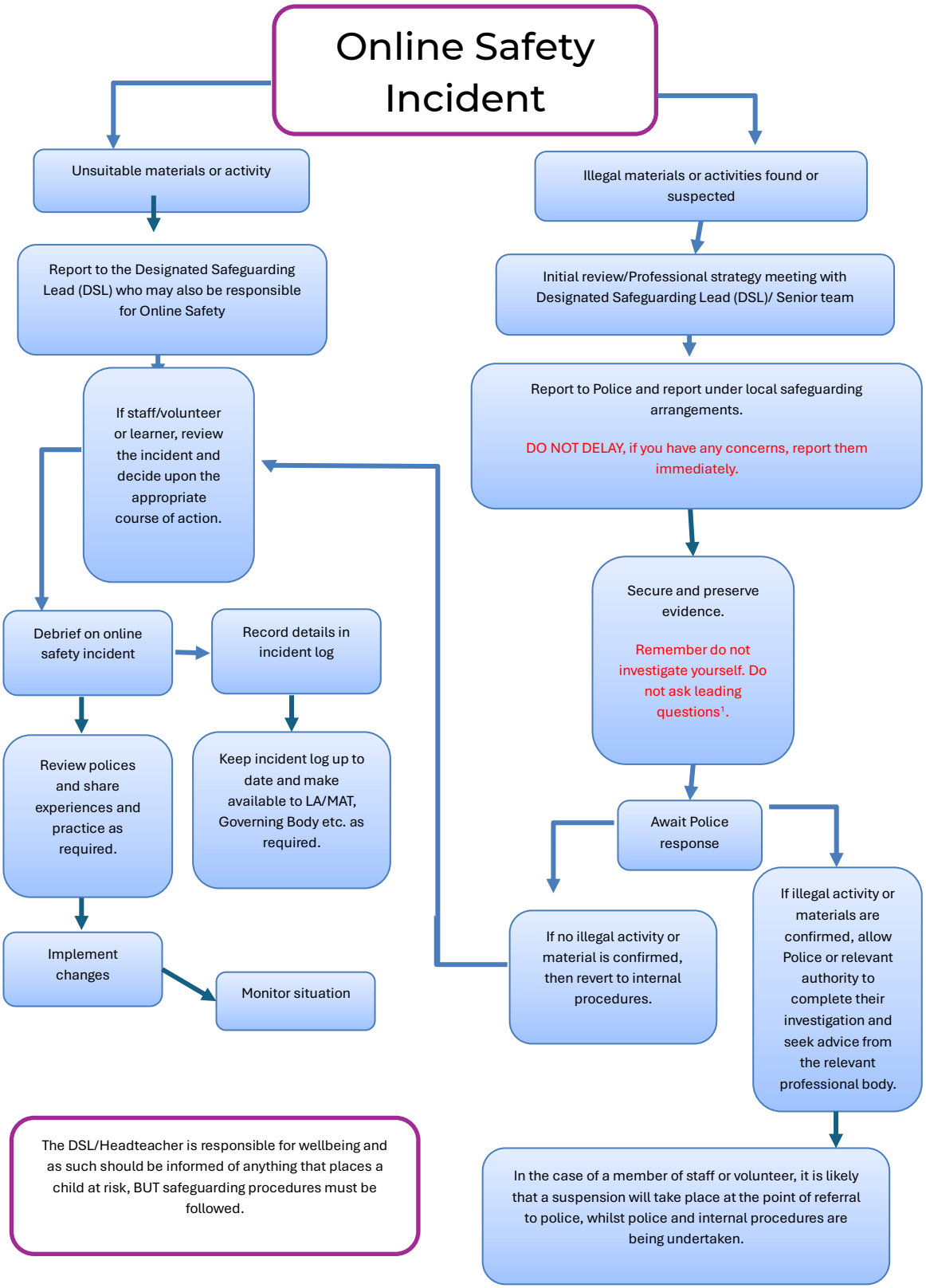
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those 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
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
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 professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The 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.

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	X	

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X				X				
Unauthorised use of digital devices (including taking images)	X								
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 HWB Champions 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.
- 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
- 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

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:

School Online Safety Policy Template Appendices

Appendices

A3 - Learner Acceptable Use Agreement Template – for younger learners (Explorers/ Adventurers)

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

Appendix 3 Staff (and Volunteer) Acceptable Use Policy Agreement

Ysgol Ty Coch
ICT Acceptable Use Policy

This ICT Acceptable Use Policy (AUP) applies to all Ysgol Ty Coch staff (including temporary and associate staff), contractors, visitors and students of Ysgol Ty Coch, and to those using and/or accessing any element of Ysgol Ty Coch ICT infrastructure, systems and services, from on or off campus.
The use of the Ysgol Ty Coch resources is a privilege, not a right. The privilege of using the technology resources provided by Ysgol Ty Coch is not transferable or extendible by staff or students to people or groups outside the school and terminates when a member of staff or pupil is no longer a member of staff or enrolled at Ysgol Ty Coch .
The purpose of this policy is to protect Ysgol Ty Coch , its staff, students, partners and those using our IT facilities from illegal, inappropriate or damaging actions. It is also designed to ensure that all users are aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. Ysgol Ty Coch IT infrastructure, systems and services are to be used for academic and business purposes in serving the interests of the School in the course of its normal operations. It is the responsibility of every Ysgol Ty Coch IT user to read and adhere to this AUP and applicable UK laws. Infringements and breaches of these regulations may result in disciplinary or legal action.

2. School, staff and student responsibilities
2.1 School responsibilities are to:
o Provide Internet and email access to its students.
o Provide Internet blocking and web filtering of inappropriate content.
o Provide network data storage areas.
o Ysgol Ty Coch mangers reserve the right to review, monitor, and restrict information stored on or transmitted via Ysgol Ty Coch 's owned equipment and to investigate inappropriate use of resources.
o Provide staff guidance to aid students in doing research and help assure pupil compliance of the acceptable use policy.
2.2 Staff and Students are responsible for:
o Using computers/devices in a responsible and ethical manner.
o Obeying general school rules concerning behaviour and communication that apply to Mobile Device / computer use.
o Using all technology resources in an appropriate manner so as to not damage school equipment.
o Helping Ysgol Ty Coch to protect our computer system/devices by contacting ICT Support about any security problems they may encounter.
o Monitoring all activity on their account(s).
o Staff and Students should always turn off and secure their Mobile Devices after they are done working to protect their work and information; this includes restricting access to their device using a pin code. Again the ICT Support Team can assist you on this.
o If a member of staff or pupil should receive email containing inappropriate or abusive

language or if the subject matter is questionable, he/she may be asked to print a copy and submit a copy to the ICT Support Team or Senior Leadership Team.
2.3 Staff and Students Activities Strictly Prohibited:
o Illegal installation or transmission of copyrighted materials
o Any action that violates existing policies or public law
o Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
o spamming other users or sending mass or inappropriate emails
o Gaining access to other pupil's accounts, files, and/or data
o Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity
o Use of anonymous and/or false communications such as MSN Messenger, Yahoo Messenger
o Students are not allowed to give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, auction websites, email, etc.
o Participation in credit card fraud, electronic forgery or other forms of illegal behaviour. o Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
o Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.

3. Unacceptable Use
Ysgol Ty Coch's ICT and the network infrastructure may not be used for any of the activities described below:

3.1. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
3.2. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
3.3. Creation or transmission of material with the intent to defraud.
3.4. Creation or transmission of defamatory material.
3.5. Creation or transmission of material such that this infringes the copyright of another
person or company.
3.6. Creation or transmission of unsolicited bulk or marketing material to users of networked
facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
3.7. Deliberate unauthorised access too networked facilities or services.
3.8. Deliberate activities having, with reasonable likelihood, any of the following characteristics:

- wasting staff effort or networked resources; o corrupting or destroying other users' data;
- violating the privacy of other users;

- disrupting the work of other users;
- denying service to other users;
- continuing to use an item of software or hardware after ICT Services has requested that use cease;
- other misuse of Ysgol Ty Coch ICT infrastructure, services and resources, such as the introduction of "viruses" or other harmful software.

4. **Mobile Devices**

4.1. All mobile devices remain the property of Ysgol Ty Coch unless the Head teacher has given authorisation for their ownership to be transferred.

4.2. All mobile devices will have their serial numbers logged before they are distributed so they can be added to the schools resource management system.

4.3. All mobile devices are required to have both Casper Suite and Meraki 'security profiles'

installed on them. If the device runs an operating system that does not run these security programs replacement software may be installed to fulfill these security obligations. Both of these pieces of software enable the ICT support team / remote wipe to track devices and their use if they are stolen, lost, misplaced or misused in any other way.

4.4. The tracking capabilities of this software will only be used after the head teacher has given written permission for a specified senior network administrator to administer and access this function.

4.5. Any member of staff found to have removed these 'security profiles' may have their device confiscated and possibly face disciplinary proceedings.

4.6. Staff members are responsible for the general care of the mobile device issued by the school.

4.7. Staff should follow the manufactures instructions when cleaning their device.

4.8. Cords and cables must be inserted carefully into the Mobile Device to prevent damage.

4.9. Any devices that have been damaged must be taken to the ICT Support department for

Immediate evaluation.

4.10. Mobile Devices must remain free of any writing, drawing, stickers, or labels that are not

the property of Ysgol Ty Coch .

4.11. Your Mobile Device must never be left in an unlocked locker, unlocked car or any unsupervised area.

4.12. Mobile Devices must be brought to school each day in a fully charged condition. Staff need to charge their Mobile Device each evening using the official charging cable provided with their device.

5. Carrying Mobile Devices

The protective cases provided with Mobile Device has sufficient padding to protect the Mobile Device from normal treatment and provide a suitable means for carrying the device within the school. The guidelines below should be followed:

5.1. Mobile Devices should always be within the protective case when carried.

5.2. Some carrying cases can hold other objects (such as folders and workbooks), but these must be kept to a minimum to avoid placing too much pressure and weight on the Mobile Device screen.

6. Device & Screen Care

6.1. The Mobile Device screens can easily be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.
6.2. Do not lean on the top of the Mobile Device.
6.3. Do not place anything near the Mobile Device that could put pressure on the screen.
6.4. Do not place anything in the carrying case that will press against the cover.
6.5. Clean the screen with a soft, dry cloth or anti-static cloth.
6.6. Do not "bump" the Mobile Device against lockers, walls, car doors, floors, etc. as it may damage the screen
6.7. Loaned Mobile Devices may be issued to staff or students when they leave their Mobile Device for repair with ICT support or an external company. There may be a delay in getting a temporary loan device, should the school not have enough to loan.
6.8. Staff should always keep their device in the case provided by the ICT department. Damages caused when the device has been removed from the case may need to paid for by the individual member of staff.
6.9. Screensavers/Background photos
6.10. Inappropriate media may not be used as a screensaver or background photo.
6.11. Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols or pictures will result in disciplinary actions.

7. Storage, Sound, Music, Games, Apps or Programs

7.1. Music is allowed on the Mobile Device and can be used at the discretion of the staff. At least 1.5 gigabytes of memory must be kept free for new apps to be installed, pictures to be stored, security profiles to be stored or other school functions to be applied.
7.2. Mobile Devices designated to students or classes, iTunes accounts will be managed by ICT Support. That will include the purchasing of any apps or configurations. 7.3. Designated staff members will have access to the media server to stream music to their device for pupils use i.e. in sensory rooms.
7.4. Mobile devices must have enough memory space reserved by the individual user to perform the desired function as directed by the teacher, head of department or senior leadership team.

Saving to the Mobile Device /Home Directory

8.1. Staff and students may save work to the home directory on the Mobile Device. Storage space will be available on the Mobile Device BUT it will NOT be backed up in case of re-imaging. It is the staffs' responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Mobile Device malfunctions are not an acceptable excuse for not submitting work.

Network Connectivity

9.1. Ysgol Ty Coch can make no guarantee that their network will be up and running 100% of the time.

9.2. In the rare case that the network is down, Ysgol Ty Coch will not be responsible for lost or missing data.

Software on Mobile Devices

10.1. Certain Mobile Devices will have restrictions that will prevent users deleting and installing apps, and configuring system settings. In these situations ICT Support will manage the content of the Mobile Device.
10.2. The software/apps originally installed by Ysgol Ty Coch must remain on the Mobile Device in usable condition and be easily accessible at all times.
10.3. From time to time the school may add software applications for use when there are particular pupil requirements. Periodic checks of Mobile Devices may be made to ensure that staff have not attempted to remove required software.

Inspection

11.1. Staff or students may be selected at random to provide their Mobile Device for inspection to ensure that they are following the protocol laid out in this acceptable use policy.

Procedure for re-loading software

12.1. If technical difficulties occur or illegal software is found the Mobile Device will be restored from backup. The school does not accept responsibility for the loss of any software, documents, media or other content deleted due to the re-formatting and re- imaging process.

Software upgrades

13.1. Upgrade versions of licensed software/apps are available from time to time. Staff or students may be required to check in their Mobile Device for periodic updates, synching and or backing up.

Mobile Device Damage

14.1. Staff are responsible for the care and security of any device issued to them by the school. In the case of iPod Touches and iPads staff will be liable for damage to or total loss of the device if it is damaged beyond repair. The only exception will be damage incurred in the course of duties whilst in work. All loss, theft or damage MUST be reported to the ICT Team immediately and a behavior report must be uploaded to the schools behavior watch system using the word ‘damaged
14.2. All mobile devices are the property of Ysgol Ty Coch unless the head teacher agrees to pass on ownership of the device.

Security

15.1. iPod and iPad devices must also be configured to automatically initiate a local wipe after 10 failed passcode attempts. This will protect against brute force attempts to gain access to the device and protect sometimes sensitive data like emails. When enabled iPods and iPad’s will automatically wipe the device after 10 failed passcode attempts. It is vitally important to back up your device to the ‘cloud’ or a local iTunes account.

Mobile Device Identification

16.1. Pupil and staff Mobile Devices will be labelled in the manner specified by the school. Mobile Device can be identified by a record of the devices serial number.

Storing Your Mobile Device

17.1. When staff or students are not using their Mobile Device, they should be stored in lockable cabinets, behind fobbed / locked doors or in their staff locker. It is recommended that staff use either a lock provided by the school or leave their device with the ICT Support Team.
17.2. Under no circumstances should Mobile Device be left in unsupervised areas. Unsupervised areas include the school outside grounds, unlocked classrooms, the dining room, library, toilets and hallways. Any Mobile Device left in these areas is in danger of being stolen. If a Mobile Device is found in an unsupervised area, it will be taken to ICT Support Services, Senior Management Team or the Administration Offices.
17.3. Ysgol Ty Coch staff should take appropriate security measures to protect the laptop and all its peripherals. When unattended, the laptop should be stored in a secure locked location.

Access to Networks and Services

18.1. Registered network users must not intentionally or recklessly use the name of Ysgol Ty Coch or any of its members in such a way that either by content or expression it brings the good name of Ysgol Ty Coch into disrepute. Where the Ysgol Ty Coch network is being used to access another network or service, any abuse of the acceptable use policy of that network will be regarded as unacceptable use.
18.2. Any deliberate activity as described in Section 2 of this AUP, where applied to a user of that network, will also be regarded as unacceptable. Any activity that is likely to damage the reputation of Ysgol Ty Coch , and/or of Ysgol Ty Coch ICT infrastructure and services, will also be regarded as unacceptable may result in disciplinary or legal action

.

Research

19.1. It is recognised that, in the course of their work or research, registered users of Ysgol Ty Coch may have a requirement to create, transmit or receive material that would normally be defined as unacceptable use. In the case of properly authorised, supervised and lawful research purposes it is acceptable to do so, following the completion of Ysgol Ty Coch 's Acceptable Use Policy Waiver form. Those applying for a waiver should complete the form, and obtain the authorising signature from the Senior Management Team, if deemed appropriate. Individuals must understand that an AUP waiver does not sanction the committal of acts that are illegal.

Personal Use

20.1. Ysgol Ty Coch permits the reasonable personal use of its ICT facilities, infrastructure and services as a privilege, not a right, on the understanding that personal use:
20.2. is lawful and complies with Ysgol Ty Coch 's rules, regulations, policies and procedures.
20.3. is not detrimental to the main purpose for which the facilities are provided;
20.4. does not interfere with the performance of an individuals duties;
20.5. does not take priority over an individual's work or learning responsibilities;
20.6. is not of a commercial or profit-making nature, or for any other form of personal financial gain;
20.7. is not connected with any use or application that conflicts with an individual's obligations, contractual or otherwise, to Ysgol Ty Coch ;
20.8. does not incur unwarranted expense on Ysgol Ty Coch ;

20.9. does not in any way have a negative impact on Ysgol Ty Coch .
20.10. For the purposes of monitoring, all Ysgol Ty Coch email is deemed to be business related communications, unless specifically identified as 'Personal' in the title / subject line.

21. Email, Forums, Blogs and Online Networking Services
Users should be mindful of the content of electronic messages or posts, including those on virtual learning environments and social networking sites, as incorrect or improper statements can give rise to personal or corporate liability. Deletion of inappropriate content does not necessarily mean that an electronic message or post is irretrievable. Electronic messages and posts may be read by others, content could it find its way into the public domain, and may be disclosed (and is admissible) in legal proceedings.

The following activities are not permitted:
21.1. Posting of obscene and/or offensive comments, or otherwise objectionable material (including but not limited to libellous, unlawful, defamatory, racist, sexist, homophobic, harassing, harmful, abusive, threatening, or visual sexual references);
21.2. Posting of material that may violate, plagiarise, or infringe on the rights of third parties including copyright, trademark, trade secret, privacy, personal, publicity, or proprietary rights;
21.3. Posting of material that intentionally or recklessly uses the name of Ysgol Ty Coch or any of its members in such a way that either by content or expression it brings the good name of Ysgol Ty Coch into disrepute.
21.4. Posting of material that directly contravenes the Data Protection Act 1998 in that it is sensitive or personal and is owned by individuals, pupils, parents, governors, school staff or other relevant third parties.

Staff email use:
Ysgol Ty Coch 's Office 365 email system is not normally monitored and users are free to use the system to share information and ideas. The management of Ysgol Ty Coch expect the use of the system to comply with the legal and professional responsibilities described in this policy and within all UK law.
21.5. The senior leadership team may at times use the Office 365 portal or any other means to monitor the use of email by employees if users are suspected of sharing illegal, inflammatory, slanderous, defamatory or bullying content within their email messages. Using the Office 365 portal these emails may be tracked, reviewed and printed if requested by the head teacher.
21.6. Employees found to be in breach of this policy may face disciplinary action in line with the code of conduct or practice.
21.7. Ysgol Ty Coch keeps email messages for up to seven year and can be reviewed within this time at any point to serve as part of an investigation.
22. Liability
22.1. In using Ysgol Ty Coch ICT facilities and / or services each user agrees that Ysgol Ty Coch shall have no liability for the loss or corruption of any user file or files, information or data; and/or the loss or damage to any user owned equipment, devices, systems or other assets resulting from the individual's use of Ysgol Ty Coch ICT infrastructure and services.
22.2. Ysgol Ty Coch shall not in any event be liable for any damages, costs or losses

(including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of these services, or with any delayed access to, or inability to use these services.

23. Compliance and Illegal Material

23.1. Under UK law Ysgol Ty Coch has a legal responsibility for the content and nature of all materials stored on, accessed and/or transmitted via Ysgol Ty Coch ICT infrastructure, and has therefore adopted standard procedures to monitor and verify any report of potentially illegal material. Ysgol Ty Coch will not endorse the committal of acts that are illegal, and where illegal material is suspected as having been viewed, stored or transmitted via Ysgol Ty Coch ICT infrastructure, the information will be immediately forwarded to the Police for investigation.

24. User Ids and Passwords

24.1. The use of another individual's User ID and password is not permitted under any circumstances. Registered users must not disclose their passwords, and must take all reasonable precautions to ensure that their password remains confidential. Any individual who discloses their password to another will be held responsible for any improper actions committed under that User ID and, in circumstances where further breaches of the AUP occur, accountability may fall equally on the holder of the account, as on the individual using the account at the time.

24.2. Where a temporary password is issued, it must be changed immediately to a secure password known only to the individual; failure to do so will create a security risk. Registered users should select a secure password by using a combination of alphabetic and non-alphabetic characters; avoiding the use of real names or words, or the use of sequences of numbers or letters.

25. Logging and Monitoring

25.1. As defined under The Regulation of Investigatory Powers Act 2000, Ysgol Ty Coch monitors electronic communications, telecommunications systems and activity across the ICT infrastructure and network services for the purpose of recording evidence of transactions, ensuring regulatory compliance, detection of crime or unauthorised use, and for system monitoring to ensure the operation effectiveness of ICT systems and services.

25.2. Ysgol Ty Coch systems automatically record all registered user account logins, system accesses, and email and Internet activity on and across Ysgol Ty Coch ICT infrastructure. These records may also be used as part of a disciplinary or criminal investigation.

26. Security, Privacy and Access

26.1. Individuals should be aware that electronic communications and transactions are vulnerable to potentially malicious activity and security breaches during transmission and can be intercepted, read, lost, redirected or amended. It is the responsibility of the individual to appropriately check communications and transactions, files and data, to ensure it is from an identifiable and reliable source. Whilst Ysgol Ty Coch shall take reasonable measures to reduce the risk of malicious activity and/or vulnerable to security breaches, Ysgol Ty Coch shall not be held responsible for any loss or damage resulting from an individual's use of, and/or access to, Ysgol Ty Coch ICT infrastructure and services.

26.2. All registered users need to be aware that the automated monitoring of their usage may reveal sensitive personal data about the individual. By using and/or accessing Ysgol Ty Coch ICT infrastructure and services, registered users consent to Ysgol Ty Coch processing any sensitive personal data (inline with the principles of the Data Protection

Act) which may reveal unacceptable or illegal activity. Access to another user's home directory files is not permitted without either the individual's explicit consent or, if this is unavailable, the formal consent of a member of the Senior Management Team. Individuals will be informed if access has been granted during their absence. Access to home directories may be granted as part of a disciplinary or criminal investigation.

27. Software Licensing and Copyright Expectations

27.1. The use of unlicensed software is illegal and, unless formally advised to the contrary, it is to be assumed that all software products are subject to Copyright Law. Use of software products are limited to the purposes defined in the licensing agreement - typically for teaching, research, personal educational development, administration and management of Ysgol Ty Coch . In many cases, software licenses may only be used on ICT equipment covered by that specific license agreement. Registered users of Ysgol Ty Coch , and users of Ysgol Ty Coch ICT infrastructure and services, must not copy or distribute copies of any Ysgol Ty Coch licensed software.

27.2. The downloading, storing or transmitting of copyrighted material, including electronic texts, music, operating systems and video files, is not permitted (see Section 2.5). It is also illegal under the 'Copyright, Designs and Patents Act (1988)' to reuse copyrighted content without the documented permission of the copyright holder. Ysgol Ty Coch will perform checks across our ICT systems and services for peer-to-peer file-sharing software and files suspected to contain copyrighted material. Where copyrighted material is suspected, the user's account will be disabled and the files removed pending further investigation. Disciplinary and/or legal action may follow.

Legal Propriety

27.3. Employees must comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a member of the ICT Support Services.

27.4. Plagiarism is a violation of Ysgol Ty Coch rules, procedures and policies. Give credit to all sources used in a document whether quoted or summarised. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

27.5. Use or possession of hacking software is strictly prohibited and violators and may result in criminal prosecution or disciplinary action by Ysgol Ty Coch.

28. Software Installations and Executable Files

28.1. Registered users are not permitted to install any software or executable files (including alterative or parallel operating systems) on Ysgol Ty Coch ICT devices or infrastructure without the prior formal consent of a senior ICT Services representative. ICT Services perform regular checks and where files or software of this type are found, the user's account will be disabled and the files removed pending further investigation, and disciplinary action may follow.

28.2. All uses of Ysgol Ty Coch ICT infrastructure must consult members of the IT department before updating their machine to use a newer version of their operating system or newer versions of software.

29. Personal / User Owned ICT Devices

29.1. All Ysgol Ty Coch staff are permitted to use personal / user owned ICT devices on Ysgol Ty Coch premises, and to connect to the 'wireless' network provided by Ysgol Ty Coch . However, under no circumstances should personal / user owned ICT devices be connected to Ysgol Ty Coch 'wired' network infrastructure.

29.2. Before any personal electrical device is connected into the institutional electrical distribution system, individuals should ensure they are able to demonstrate that their equipment has been the subject of a formal, visual inspection as defined by the Electricity at Work Regulations Approved Code of Practice. Individuals using personal user owned ICT devices to access or connect to any element of Ysgol Ty Coch ICT infrastructure and services from on or off school premises, do so on the understanding that this is done at the individual's own risk. Ysgol Ty Coch accepts no responsibility for any loss or damage to user owned ICT devices, files, information or data.

30. Equipment Malfunction, Loss, Damage or Stolen

30.1. In case of malfunction, ICT Services will try to repair or replace the item.
30.2. All equipment must be left operational and in good working order after each class or usage. Users assume full responsibility for damage or loss of equipment due to negligence or abuse. If a device is damaged beyond repair the user may be pursued for financial liability, as individuals are responsible for loss or damage to Ysgol Ty Coch ICT equipment.
30.3 Intentional vandalism or theft of equipment will be investigated by the senior leadership team and may be forwarded to the police.

31. Removal of ICT Equipment, Software or Information

The removal of Ysgol Ty Coch School ICT equipment, software or information is not permitted without prior formal authorisation from the appropriate Ysgol Ty Coch authority. Ysgol Ty Coch ICT-related 'assets' removed without authorisation may be viewed as being stolen and may result in disciplinary proceedings.

32. Suspension of Access

All users have the responsibility to adhere to this AUP. Where a breach has been identified, or infringement suspected, suspension of access to ICT facilities will be immediately implemented to enable the incident to be investigated. Where it has been proven that a breach has occurred, formal disciplinary proceedings may be implemented.

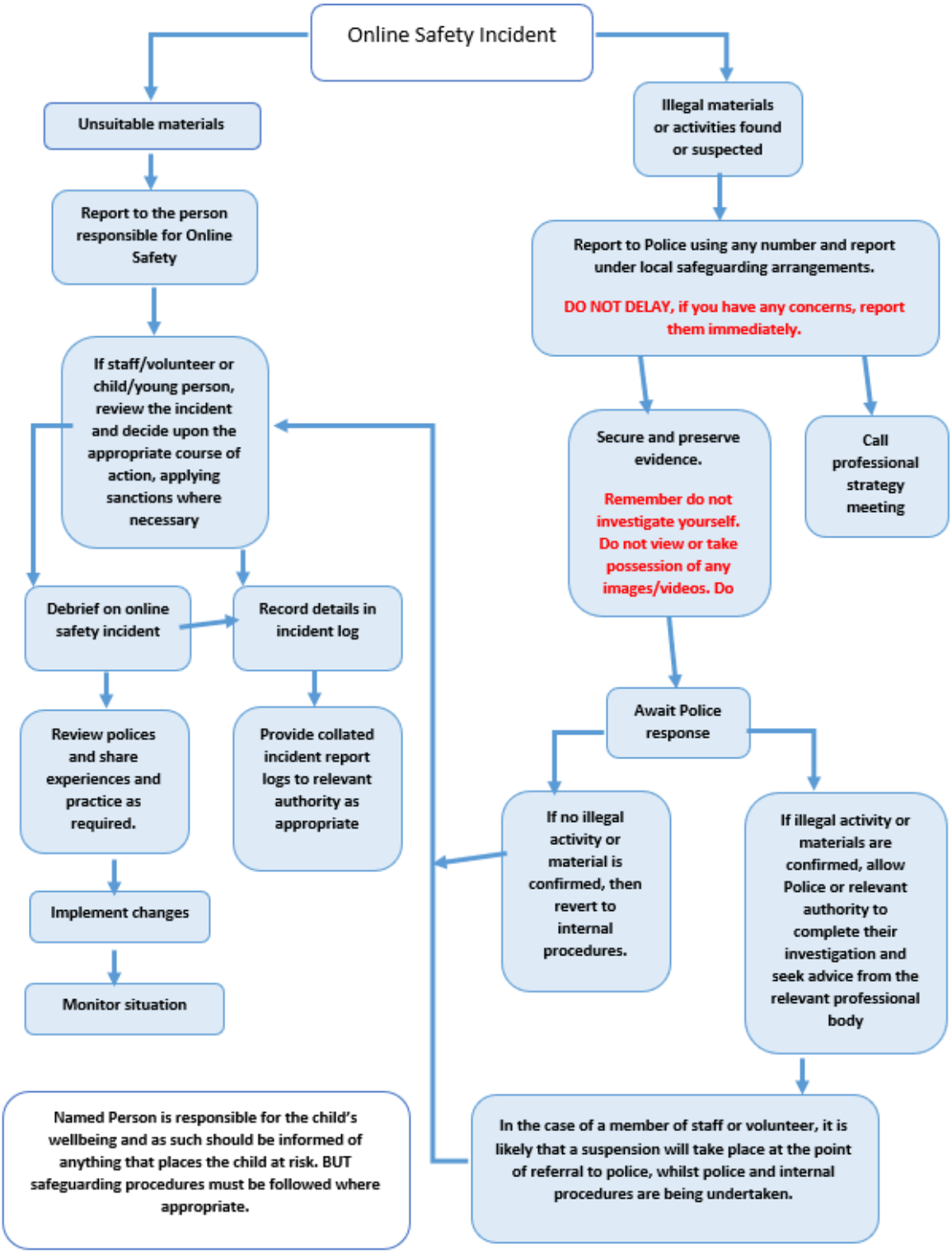
Appendix A Legislation

Applicable laws, primary Acts of Parliament and policies, which relate to and/or govern the provision and use of ICT facilities include:
Regulation of Investigatory Powers Act 2000 Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Copyright, Designs & Patents Act 1988
Copyright and Trademarks (Offences and Enforcement) Act 2002
The Telecommunications Act (1984)
The Electronic Communications Act (2000) Obscene Publication Act 1959 & 1964 Protection of Children Act 1978
Human Rights Act 1998
The Defamation Act (1996)
Police and Criminal Evidence Act 1984
Police and Justice Act 2006
Prevention of Terrorism Act 2005
Terrorism Act 2006

This list is not exhaustive and may be subject to change.
I agree to abide by the above

30.1. Any ICT equipment that malfunctions, is lost, damaged or is stolen must be reported to the school's Business Manager (or a delegated member of staff as directed by the Business Manager) as soon as possible.
Print Name: Signed: Date:
…… ……
……

A9 Responding to incidents of misuse – flow chart



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_Headteachers_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, RCT corporate emails and other approved platforms/devises such as Hwb, TEAMS and mobile phones. Video calls to people outside the school 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.