Trallwng Infant School

Online Safety Policy

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

Version: [1}

Date created: [06/010/2021]

Next review date: [06/10/2022]

Scope of the Online Safety Policy

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

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

Trallwng Infant 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/education practitioners/support staff/technical staff*
- *governors*
- *parents and carers*
- *community users*

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

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*Insert date*
The implementation of this Online Safety Policy will be monitored by:	*Becky Williams & senior leadership*
Monitoring will take place at regular intervals:	*Annually or as appropriate*
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 or as appropriate*
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:	*May 2022*
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*
- *surveys/questionnaires of:*

  - o *learners*
  - o *parents and carers*
  - o *staff.*

Policy and leadership

Responsibilities

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

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to 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 e.g. by asking the questions posed in the Welsh

---

[1]

[2]

[Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners.](#) This will be carried out by Esther Sowerby who will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

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

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

Designated Safeguarding Person (DSP)

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

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

Curriculum 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
- thehnology systems in accordance with the learner acceptable use agreement
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- 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:

- 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

Community users

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

Online Safety Group

The Online Safety Group has the following members

- online safety lead
- Designated Safeguarding Person
- senior leaders
- online safety governor
- teacher and support staff members
- learners
- parents/carers
- community representatives

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

- the production/review/monitoring of the school Online Safety Policy/documents
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage of the Digital Competence Framework
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, recent trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool.

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

Professional Standards

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

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

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies

- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- 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.

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

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

The acceptable use agreements will be communicated/re-enforced through:

- student handbook
- staff induction and handbook
- 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 visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978 N.B. Schools should refer to guidance about dealing with nudes and semi-nudes being shared.					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
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						X

● 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				
Using school systems to run a private business				X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X
Infringing copyright				X
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)				X
Creating or propagating computer viruses or other harmful files				X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X
Online gaming (educational)	X			
Online gaming (non educational)	X			
Online gambling				X
Online shopping/commerce				X
File sharing	X			
Use of social media				X
Use of messaging apps				X
Use of video broadcasting, e.g. YouTube	X			

	Staff and other adults			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	x			
Use of mobile phones in lessons		x		
Use of mobile phones in social time	x			
Taking photos on mobile phones/cameras		x		
Use of other mobile devices, e.g. tablets, gaming devices	x			
Use of personal e-mail addresses in school, or on school network		x		
Use of school e-mail for personal e-mails				
Use of messaging apps		x		
Use of social media		x		
Use of blogs	x			

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

- the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.
- users must immediately report to the nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications
- learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of digital citizenship and the need to communicate appropriately when using digital technologies.
- personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.
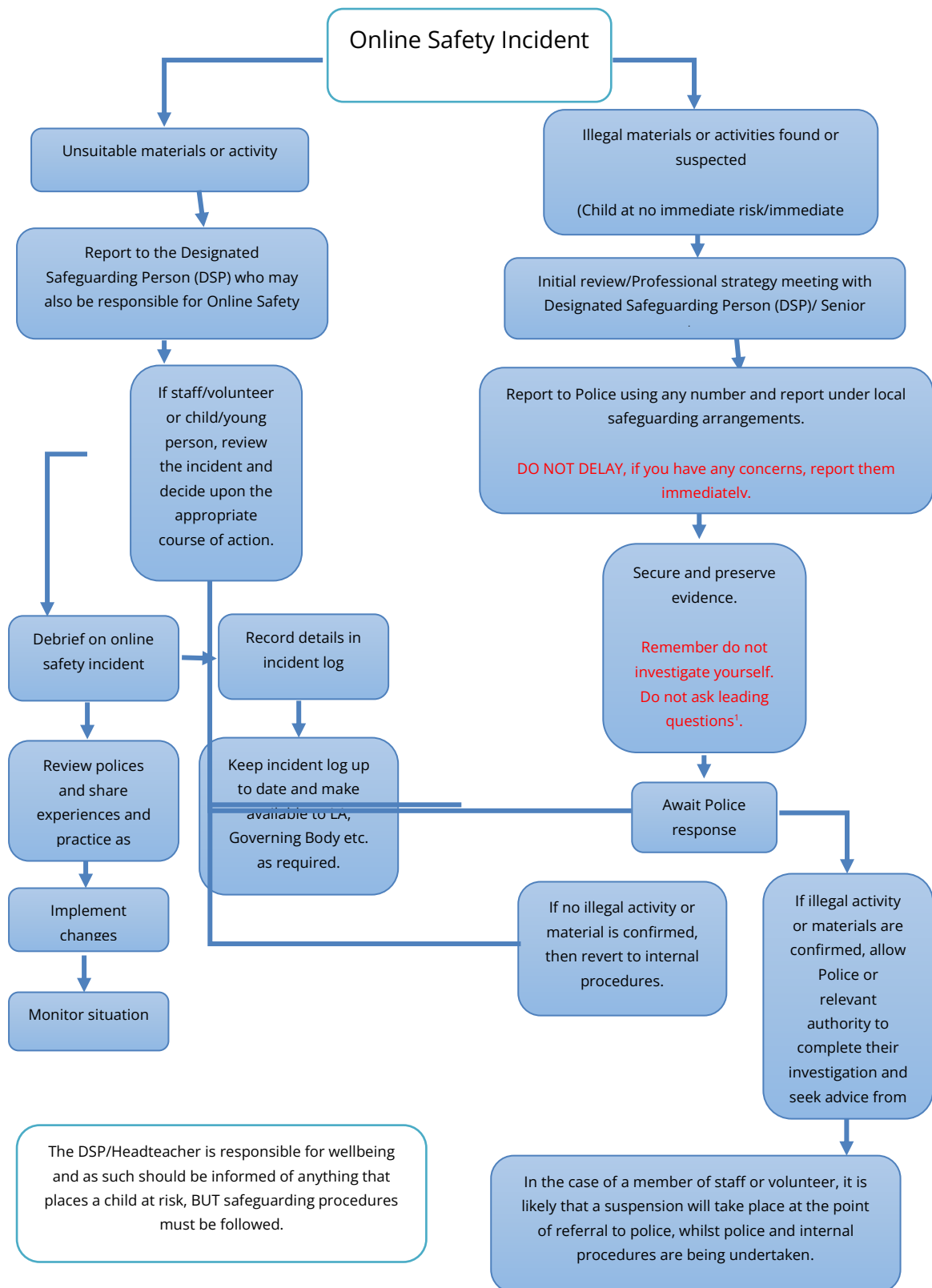
Reporting and responding

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 immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same computer for the duration of the procedure.
  - it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see above).
  - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority (as relevant)
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged in the school reporting log
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb

- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- 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*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant*

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

Online Safety Incident

Unsuitable materials or activity

Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as

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

Implement changes

Monitor situation

The DSP/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Illegal materials or activities found or suspected

(Child at no immediate risk/immediate

Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior

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

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

Secure and preserve evidence.

Remember do not investigate yourself. Do not 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

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

School actions

It is more likely that the school will need to deal with incide

nts that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Issue a warning	Further sanction, e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons.	X								
Unauthorised use of mobile phone/digital camera/other mobile device.	X								
Unauthorised use of social media/messaging apps/personal e-mail.	X								
Unauthorised downloading or uploading of files.	X								

	1	2	3	4	5	6	7	8	9
Allowing others to access school network by sharing username and passwords.	X								
Attempting to access or accessing the school network, using another learners' account.	X								
Attempting to access or accessing the school network, using the account of a member of staff.	X								
Corrupting or destroying the data of other users.	X								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X								
Continued infringements of the above, following previous warnings or sanctions.			X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X						
Using proxy sites or other means to subvert the school's filtering system.			X						
Accidentally accessing offensive or pornographic material and failing to report the incident.			X						
Deliberately accessing or trying to access offensive or pornographic material.				X					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.				X					

Staff Actions

Incidents	Refer to Headteacher/ Principal	Refer to local authority/ HR	Refer to Police	Refer to 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				
Inappropriate personal use of the internet/social media/personal e-mail	X						
Unauthorised downloading or uploading of files.	X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X					
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X						
Deliberate actions to breach data protection or network security rules.	X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X				
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X				

Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers	X						
Actions which could compromise the staff member's professional standing	X	X					
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X					
Using proxy sites or other means to subvert the school's filtering system.	X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X					
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X
Breaching copyright or licensing regulations.	X	X					
Continued infringements of the above, following previous warnings or sanctions.							X

Education

Online Safety Education Programme

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional

language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education

- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *learners should be 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*
- the online safety education programme will be regularly audited and evaluated 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*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- *the Online Safety Lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

Governors should take part in online safety training/awareness sessions through

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

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, Hwb*
- *high profile events/campaigns e.g. Safe Internet Day*
- *reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, www.saferinternet.org.uk/ www.childnet.com/parents-and-carers (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority*

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their learning platform, website, and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

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 Welsh Government Recommended web filtering standards for schools and the UK Safer Internet Centre Appropriate

(The school will need to decide on the merits of external/internal provision of the filtering service – see Appendix).

- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- *the school has (if possible) provided enhanced/differentiated user-level filtering* (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)
- *younger learners will use child friendly/age appropriate search engines e.g. SWGfL Swiggle*
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*

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

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

- physical monitoring (adult supervision in the classroom)
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*

Users are made aware, through the acceptable use agreements, that monitoring takes place.

Technical Security

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in local authority/other relevant body policy and guidance)
- 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 copies off-site or in the cloud, (this is good practice in helping to prevent loss of data from ransomware attacks)
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group)
- all users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details. Sharing of passwords or ID and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and 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 xxxxx (insert name or title) who will keep an up to date record of users and their usernames (see section on password generation in 'Technical security policy template' in the Appendix)
- the master account passwords for the school systems are kept in a secure place, e.g. school safe. It is recommended that these are secured using two factor authentication for such accounts (further guidance is available in the 'Technical security policy template' in the Appendix)
- passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length is more secure than any other special requirements such as uppercase/lowercase letters, number and special characters. Users should be encourage to avoid using sequential or chronological numbers within their passwords. Passwords/passphrases should be easy to remember, but difficult to guess or crack

- records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- (insert name or role) is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- an appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place (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 (to be described) regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail)

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[4]	Student owned	Staff owned	Staff owned
Allowed in school	X	X	X	No	Yes	Yes
Full network access	X	X	X			
Internet only						
No network access						

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*

---

[4] .

- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

Social media

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

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to follow the professional conduct set out by the General Teaching Council Wales (GTCW) and respect learners, their families, colleagues and the school.

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

- ensuring that personal information is not published
- 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
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

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

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

Monitoring of public social media
- As part of active social media engagement, the school will 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
- 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 related to digital and video images and will implement policies to reduce the likelihood of the potential for harm

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

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

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

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

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

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

Data Protection

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

The school follows the Local Authority Data Protection Policy and:

- implements the data protection principles and is able to demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- 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 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
- 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
- As a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests
- Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

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

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

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- will not transfer any school personal data to personal devices.
- 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
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

Appendix

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

The Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe Cymru online safety self-review tool:

Acknowledgements:

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