St Mary's Catholic Primary School

Online Safety Policy

Updated January 2025

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

Name (Chair of Governors)	Mrs Esther Bennington
Signed:	
Date of next review	Dec 2026

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Mary's Catholic Primary 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 devices on the school site (where allowed).

St Mary's Catholic Primary 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 headteacher/senior leaders, governors and digital leaders.

Schedule for development, monitoring and review

The implementation of this Online Safety Policy will be monitored by:	*The online safety lead and senior leadership team.*
The Online Safety Policy will be reviewed every two years 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:	*Dec 2026*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Rebecca Phillips- LA Safeguarding Officer*

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

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting

inappropriate online behaviours, concerns and misuse as soon as these become apparent.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to an appropriate member of the senior leadership team.
- The headteacher and senior leadership team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that all staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

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 Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners. This will be carried out by the Safeguarding governor 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[1]

as part of their Safeguarding governor role to include:

- regular meetings

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

- 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*

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

Mrs Acton, Headteacher, is the named person responsible for Safeguarding and Mrs Gillett, KS 2 Phase Leader

The online safety lead will:

- work closely on a day-to-day basis with the other Designated Safeguarding Persons (DSP)
- 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 teachers 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 and create a log of incidents to inform future online safety developments
- identify sources of training and advice for staff/ governors/ parents/ carers/ learners
- liaise with LA technical staff, pastoral staff and support staff (as relevant)

- meet regularly with the online safety governor (Safeguarding) to discuss current issues, review (anonymised) incidents
- attend relevant governing body meetings/groups
- liaises with the local authority/relevant body

Designated Safeguarding Person (DSP)

Mrs Acton is the Designated Safeguarding Person who is trained in online safety issues and is 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 Leaders

Teachers will work collaboratively to develop a planned and coordinated online safety education programme. This will be provided through

- a discrete programme
- the Digital Competence Framework
- relationships and sexuality education
- 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 the headteacher/Designated safeguarding leaders for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners, parents and carers should be on a professional level and only carried out using official school systems and devices
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites that are checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to Live-streaming and video-conferencing: safeguarding principles and practice guidance, which outlines key considerations to ensure safe practice when live-streaming.
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The local authority is the managed technical service provider.

The LA is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy in order to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets the required online safety technical requirements as identified by the local authority, Welsh government via the Education Digital Standards or other relevant body
- users may only access the networks and devices through a properly enforced password protection policy
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of the technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported to Mrs Acton 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

Learners

- are responsible for using the school digital technology 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
- will be expected to know and follow school Online Safety Policy
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

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
- Parents and carers can find information to support their understanding of online safety on our school website and the parent e-safety website, also newsletters, resources from Hwb and our learning platform, as well as details of national and 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
- appropriate use of digital and video images taken at school events
- access to the school website/ social media platforms

Professional Standards

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

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

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

Acceptable use

Acceptable use agreements

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 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.

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

- staff handbook
- digital signage
- communication with parents/carers
- built into education sessions

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

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 nude and semi-nude images (sometimes referred to as 'sexting') - Sharing nudes and semi-nudes: Responding to incidents and safeguarding children and young people.					X
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.					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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 – read more about this: NCA Cyber Choices Programme					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

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	X				X			
Online shopping/commerce	X				X			
File sharing	X				X			
Social media	X				X			
Messaging/chat	X				X			
Entertainment streaming e.g. Netflix, Disney+	X				X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok	X				X			
Mobile phones may be brought to school	X							X
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school					X			
Taking photos on mobile phones/cameras					X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			

Use of personal email in school, or on school network/wi-fi	X				X			
Use of school email for personal emails	X				X			

**Personal calls/ texts are permitted in some circumstances e.g. emergency, waiting for a call from the doctor, in these cases staff should inform a member of the SLT.

***Staff are permitted to take photos on mobile phones for professional reasons if necessary, e.g. during a school trip. if no other device is available. These should be deleted as soon as possible afterwards.

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

*The official Hwb or school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and learners should therefore use only the Hwb e-mail service to communicate with others when in school, or on school systems (e.g. by remote access)

• 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, personal 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

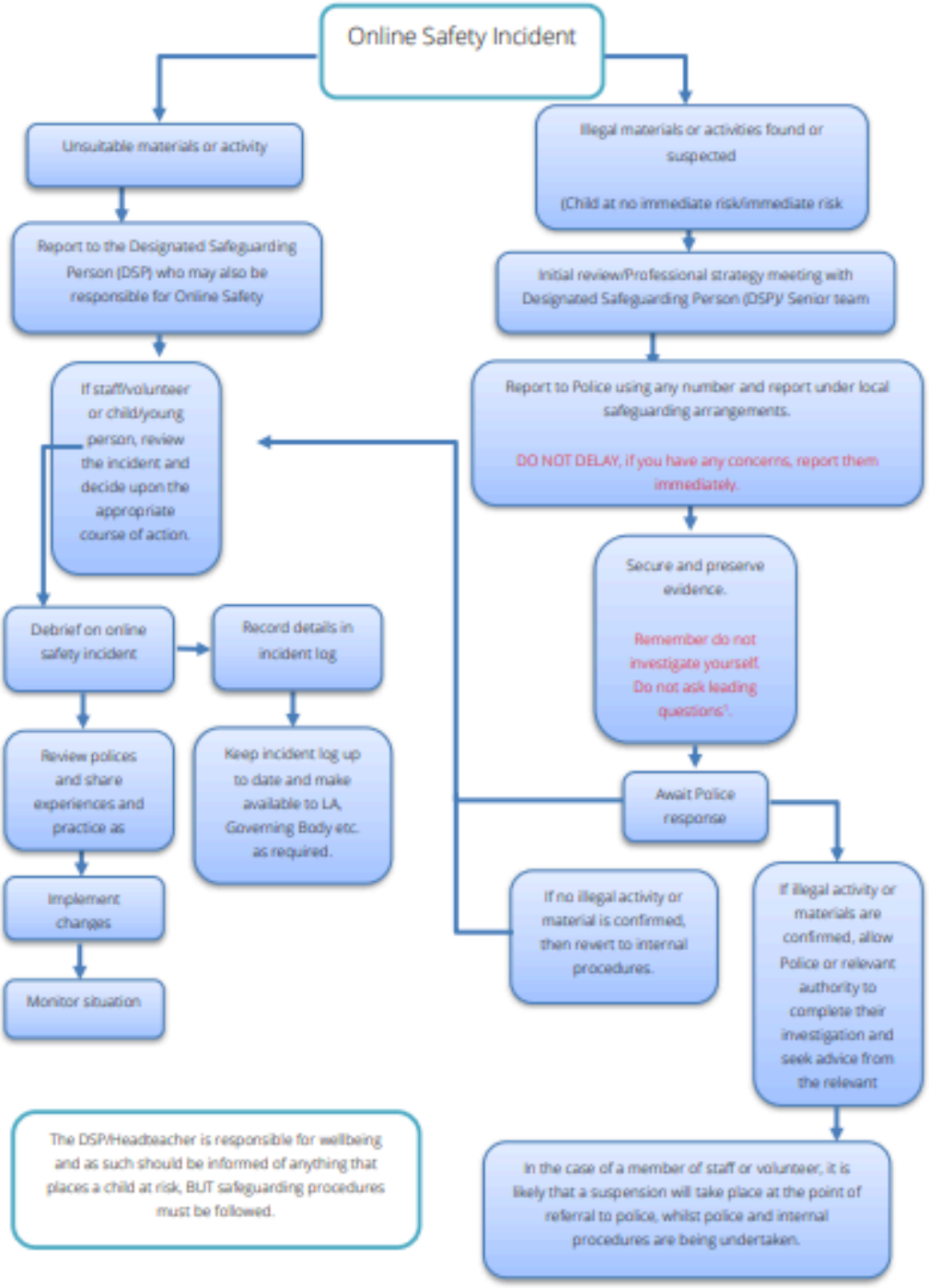
The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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 grievance 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 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, 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, Mrs Esther Bennington and the local authority
- as long as there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same computer for the duration of the procedure.
    - It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form **(except in the case of images of child sexual abuse – see above**).
    - Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those who are reporting or are affected by an online safety incident

- incidents should be logged with the Headteacher
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided to:
    - teachers 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, school website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

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


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

School actions

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

Learner Actions

Incidents	Refer to class teacher	Refer to Assistant Head or Key Stage Leader	Refer to Head	Refer to Police/ Social Worker	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			
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	X		
Corrupting or destroying the data of other users.	X	X							
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Unauthorised downloading or uploading of files or use of file sharing.	X	X							

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

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	X	X	X	X	X
Deliberate actions to breach data protection or network security rules.	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	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	X	X
Unauthorised downloading or uploading of files or file sharing.	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations.	X	X	X	X	X	X	X	X
Allowing others to access school networks by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X	X	X	X	X	X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X	X	X	X	X	X
Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers	X	X	X	X	X	X	X	X
Inappropriate personal use of digital technologies e.g. social media / personal email.	X	X	X	X	X	X	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	X
Actions which could compromise the staff member's professional standing.	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X	X	X	X	X
Failing to report incidents whether caused by deliberate or accidental actions.	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X	X

Education

Online Safety Education Programme

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

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

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/RSE/Health and Well-being AoLE) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Note: additional duties for schools under the Counter Terrorism and Securities Act 2015 require schools to ensure that children are safe from terrorist and extremist material 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

Contribution of Learners

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. This helps shape the school's approach to online safety and supports the personal development of our learners. Their ideas and involvement are valued and recognised through:

- learner feedback and opinion.
- appointment of Cyber Stewards
- 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

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 will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/GwE/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 will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions (as part of Safeguarding training), with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

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

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/providing links to appropriate websites
- 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, school website, Hwb
- high profile events/campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, The UK Safer Internet Centre, Childnet International (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

Technology

The Local Authority act as Network Manager / Technical Staff as a managed service provider.

They are responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures are implemented by the Local Authority.

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 the Local Authority and senior leaders and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours Page 22

  • the LA manages access to content across its systems for all users. The filtering provided meets the standards defined by the Welsh Government.

  • internet access is filtered for all users

  • illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider.

  • there are established and effective routes for users to report inappropriate content

  • any requests for filtering changes are made to the Local Authority
  • 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 Local Authority.

Monitoring

The school protects users and school systems through: • physical monitoring (adult supervision in the classroom) • liaison with the Local Authority if there is any issue with breach of the filter 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 by the Local Authority.
- This includes:
- 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 by the Local Authority
- 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 reviewed by the headteacher
- 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

- the master account passwords for the school systems are kept in a secure place, e.g. Bromcom MIS.
- passwords are issued by the LA or Hwb Page 23
- 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.
- The Headteacher and SLT are responsible for maintaining accurate software licence records. This includes keeping logs up to date and carrying out regular checks to ensure that the number of software installations does not exceed the number of licences purchased.
- any actual/potential technical incident/security breach should be reported to the headteacher or assistant headteacher.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place 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
- staff should not download executable files / install programmes on school devices without seeking permission from the headteacher
- personal data should not be taken off the school site e.g. USB sticks, unless safely encrypted.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage. All users

should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education covered by DCF citizenship and RSE scheme.

	School devices			**Personal devices**	
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned
Allowed in school	Yes	Yes		At times with specific permission (Mobile phones are stored by school staff during the day)	Yes
Full network access	Yes	Yes		No	No
Internet only				No	At times with specific permission
No network access				Yes	No

Personal

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

• the school permits reasonable and appropriate access to private social media sites Monitoring of public social media

• As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school

• the school 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.

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

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

- should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance and Keeping Learners Safe
- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social

networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment wherever possible. If the personal equipment of staff is used for such purposes, images should be deleted as soon as possible
- 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

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

Online Publishing

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

- Public-facing website
- Social media - Facebook, Instagram
- Seesaw
- Weekly newsletters

The school website is hosted by Schoolsays. 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 has a Data Protection policy in place.

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:

- 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.

Appendices

Digital Consent form for parents/carers
https://forms.gle/hWn1DH5UBqJkT67K6

Appendix 2- Hwb Rules and acceptable Use Agreement Pupil Acceptable Use Agreement Foundation Phase

Appendix 3 Parent & carer Acceptable use agreement -
Appendix A4 Parent and Carer Acceptable Use Agreement Templat…

https://docs.google.com/forms/d/e/1FAIpQLScJgnOC-wgfIGN7oEuVpAVqYF821tk41VYwP7l9M32OWcmmwg/viewform?usp=sharing

Appendix 4 Staff & Volunteer Acceptable Use Policy -
Supporting document 7_ Acceptable use agreement for staff and v…

Appendix 5 Record of device misuse/ internet sites Report an online issue - Hwb

Appendix 7- Reporting Log - https://forms.gle/D3Z2gbJUHHrsQ7aM8