"Working, Praying, Sharing and Learning Together"
"Gweithio, Gweddiwn, Rhannu a Ddysgu gyda'n Gilydd"

St Mary's R.C. Primary School

E-Safety Policy

Rights of the Child

Article 13	All children have the right to find out and share information and say what you think.
Article 17	All children have the right to honest information from the media that you can understand as long as it is safe.
Article 19	All children have the right to be protected from being hurt or badly treated.

February 2023

"Working, Praying, Sharing and Learning Together"
"Gweithio, Gweddiwn, Rhannu a Ddysgu gyda'n Gilydd"

E-Safety Policy

Date	Review Date	Coordinators	Nominated Governor
6/2/23	Spring 2024	Miss C Isaac & Mr M Buckley	Mr. T.R. Pritchard

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that when used correctly, Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We wish to work closely with learner pupil voice groups to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that relate to this policy.

This Policy document is drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimize risks and how to deal with any infringements of school policy.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- Mobile phones
- Digital cameras

- e-mail
- Instant messaging
- Web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

As a school, we feel it is important that we equip all our pupils with the necessary skills to prepare them for living in this highly digital world.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:
- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

Aims

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.
- To work with other schools and the local authority to share good practice in order to improve this policy.

Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by a working group made up of:

- Headteacher – Mr. T Baxter
- e-Safety ICT Coordinator – Miss. C Isaac & Mr. M Buckley
- Staff – including Teachers & Support Staff
- E-Safety Governor-
- Parents and Carers
- School Council & Digital Leaders

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

Schedule for Development/Monitoring/Review

Process for Monitoring the Impact of the Online Safety Policy

This e-Safety policy was approved by the Governing Body on:
The implementation of this e-Safety policy will be monitored by the**: HT and ICT e-Safety Coordinators.**
Monitoring will take place at regular intervals: **Annually**
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be: **Spring 2024**
Should serious e-Safety incidents take place, the following external persons / agencies should be informed: **LA Safeguarding Officer. LA Internet coordinator**

The school will monitor the impact of the policy using:

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

Roles & Responsibilities

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

Role of the Governing Body

The Governing Body are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor to include:

- Appointing a member of staff to be responsible for e-Safety.
- Delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy.
- Responsibility for ensuring that the school complies with all equalities legislation.
- Nominated a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy.
- Responsibility for ensuring funding is in place to support this policy;
- Responsibility for ensuring this policy and all policies are maintained and updated regularly;

- Make effective use of relevant research and information to improve this policy.
- Responsibility for ensuring policies are made available to parents;
- Undertaken training in order to understand e-Safety issues and procedures;
- Nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body.
- Responsibility for the effective implementation, monitoring and evaluation of this policy.
- Support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Role of the Headteacher

The Headteacher will:

- Ensure the safety and e-Safety of all members of the school community.
- Ensure all school personnel, pupils and parents are aware of and comply with this policy.
- Work closely with the Governing Body and the coordinator to create a safe ICT learning environment by having in place:
  - an effective range of technological tools
  - clear roles and responsibilities
  - safe procedures
  - a comprehensive policy for pupils, staff and parents
- The Headteacher and (at least) another member of Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator
- Ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Embed e-Safety in all aspects of the curriculum and other school activities.
- Work closely with the link governor and coordinator.

- Provide leadership and vision in respect of equality.
- Make effective use of relevant research and information to improve this policy.
- Provide guidance, support and training to all staff.
- Monitor the effectiveness of this policy by:
  - monitoring learning and teaching through observing lessons
  - monitoring planning and assessment
  - speaking with pupils, school personnel, parents and governors
  - annually report to the Governing Body on the success and development of this policy.

Role of the e-Safety Coordinator

The coordinator will:

- Be responsible for the day-to-day e-Safety issues.
- Undertake an annual e-safety audit to establish compliance with LA guidance.
- Ensure that all Internet users are kept up to date with new guidance and procedures.
- Have editorial responsibility of the school Web site and will ensure that content is accurate and appropriate.
- Ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
- Undertake risk assessments to reduce Internet misuse.
- Maintains a log of all e-Safety incidents.
- Reports all e-Safety incidents to the Headteacher.
- Ensure e-Safety is embedded in all aspects of the curriculum and other school activities.
- Lead the development of this policy throughout the school.
- Work closely with the Headteacher and the nominated governor.
- Make effective use of relevant research and information to improve this policy.
- Provide guidance and support to all staff.
- Provide training for all staff on induction and when the need arises.
- Keep up to date with new developments and resources.
- Review and monitor.
- Annually report to the Governing Body on the success and development of this policy.

Role of the Nominated Governor

The Nominated Governor will:

- Work closely with the Headteacher and the coordinator.
- Ensure this policy and other linked policies are up to date.
- Ensure that everyone connected with the school is aware of this policy.
- Undertake appropriate training.
- Report to the Governing Body every term.
- Annually report to the Governing Body on the success and development of this policy

Role of School Personnel

School personnel will:

- Comply with all aspects of this policy.
- Undertake appropriate training.
- Before using any Internet resource in school must accept the terms of the 'Responsible Internet Use' statement.
- Safe use of e-mail.
- Be aware of eBullying / Cyberbullying procedures.
- Be aware of their role in providing e-Safety education for pupils.
- Be responsible for promoting and supporting safe behaviours with pupils.
- Promote e-Safety procedures such as showing pupils how to deal with inappropriate material.
- Report any unsuitable website or material to the e-Safety Coordinator.

- Will ensure that the use of Internet derived materials complies with copyright law.
- Ensure e-Safety is embedded in all aspects of the curriculum and other school activities.
- Be aware of all other linked policies.
- Be aware of safe publication of pupil information/photographs and use of website.
- Maintain high standards of ethics and behaviour within and outside school and not to undermine fundamental British values.
- Work in partnership parents and carers keeping them up to date with their child's progress and behaviour at school.
- Implement the school's equalities policy and schemes.
- Report and deal with all incidents of discrimination.
- Attend appropriate training sessions on equality.
- Report any concerns they have on any aspect of the school community.

Staff are reminded / updated about e-Safety matters at least once a year

Role of Safeguarding Designated Person (HT/DHT)

Note: It is important to emphasise that these are safeguarding issues, not technical issues; the technology provides additional means for safeguarding issues to develop. The Safeguarding Designated Person is trained in e-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 on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Role of Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.
- Liaise with the school council.
- Take part in questionnaires and surveys.

Role of Parents/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school e-Safety Policy on the school website.

- Providing them with a copy of the learners' acceptable use agreement.
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images etc.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- Signing the parent Acceptable Use Agreement.
- Reinforcing the online safety messages provided to learners in school.
- The use of their children's personal devices in the school (where this is allowed).

Online Safety Group

This is currently being developed and will be written into policy when finalised.

Community Users

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

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

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

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

- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction and through normal communication channels (Hwb, Staff Share)
- *is published on the school website.*

Acceptable Use

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

Acceptable use agreements

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

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

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					X
Users shall not undertake	• Using another individual's username or ID and password to access data, a					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	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)					
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/awaren
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			X			
Taking photos on mobile phones/cameras			X		X			

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

Reporting and Responding

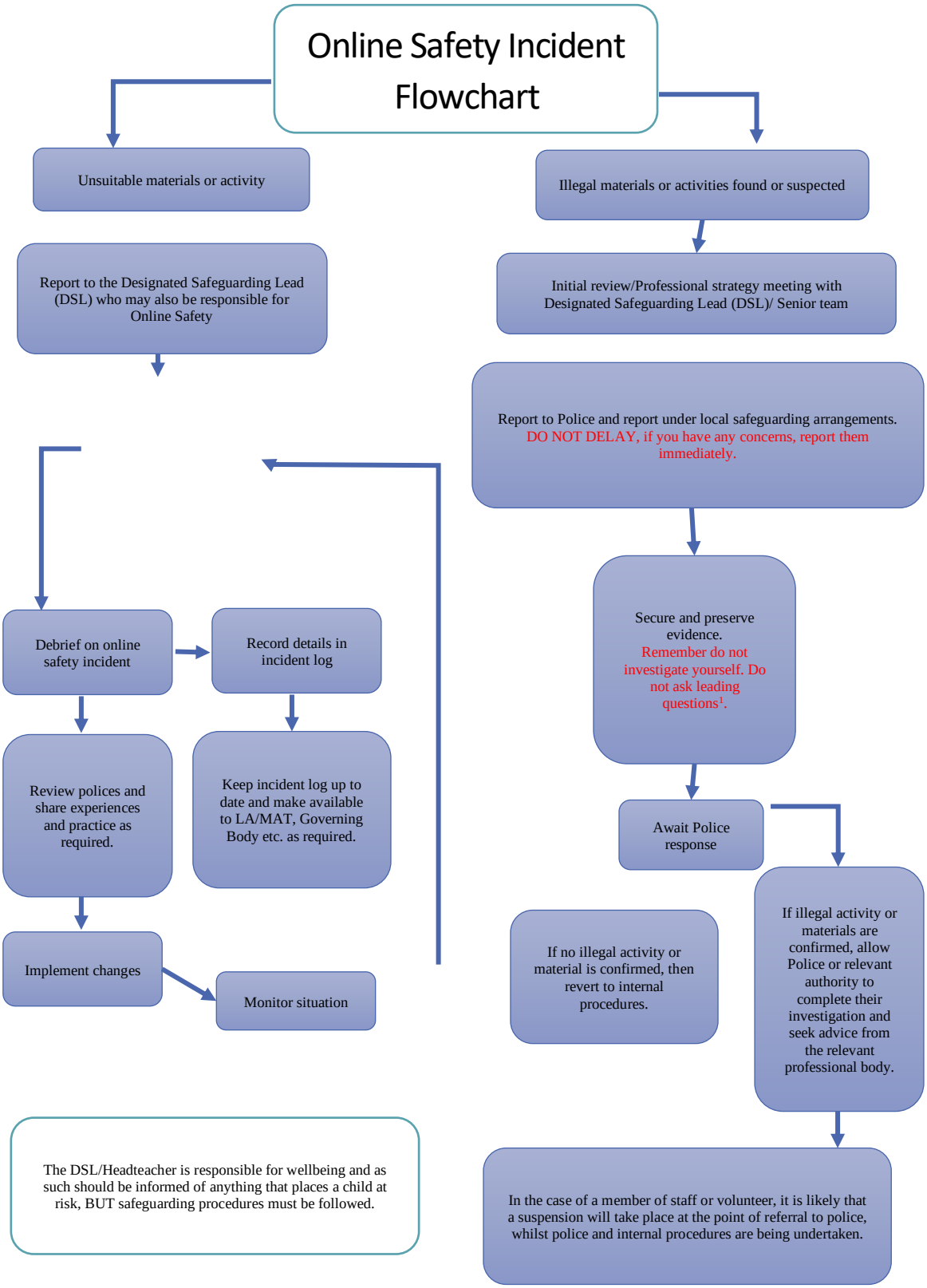
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- internal response or discipline procedures
- involvement by local authority / MAT (as relevant)
- police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.

- incidents should be logged through MyConcern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police etc.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
- *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant*
  - The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

"Working, Praying, Sharing and Learning Together"
"Gweithio, Gweddiwn, Rhannu a Ddysgu gyda'n Gilydd"

Online Safety Incident Flowchart



School Actions

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

Responding to Learner Actions

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

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

"Working, Praying, Sharing and Learning Together"
"Gweithio, Gweddiwn, Rhannu a Ddysgu gyda'n Gilydd"

Responding to Staff Actions

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

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		x						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		x						
Actions which could compromise the staff member's professional standing		x						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x				x		
Failing to report incidents whether caused by deliberate or accidental actions		x						
Continued infringements of the above, following previous warnings or sanctions.		x				x		

Online Safety Education Programme

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., Health and Wellbeing, Literacy etc
- 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 should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of Digital Leaders/School Council representatives etc.*
- *the Online Safety Group will have 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

All staff will 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 Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

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

- attendance at training provided by the local authority/MAT or other relevant organisation
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. www.saferinternet.org.uk/; www.childnet.com/parents-and-carers..*
- *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 website and social media for the wider community*

Technology

Our school has a managed ICT service provided by an outside contractor. It is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety Policy / Acceptable Use Agreements.

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

Filtering

- the school filtering is agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

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

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

- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to HT/e-safety lead.*

Technical Security

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

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- 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.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by staff who will keep an up-to-date record of users and their usernames
- passwords should be long.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Coordinators are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published.
- 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
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

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

- Public-facing website (https://www.stmarysrcbrynmawr.co.uk)
- Social media
- Online newsletters

- ClassDojo posts/messages

The school website is managed/hosted by Valley's Designs. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.
Where learner work, images or videos are published, their identities are protected, and full names are not published.

Outcomes

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

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