

# PADRE PIO CATHOLIC PRIMARY SCHOOL YSGOL GYNRADD GATHOLIG PADRE PIO

## Online Safety Policy

Online safety at Padre Pio Catholic Primary School contributes to our Mission Statement:

***'A Catholic family where we pray and learn in peace with each other. Together we take the message of Jesus to the world'***

Our aim is to provide a high-quality Christian Education based on the teachings of Christ in the Gospels, where each individual is a valued member of our community and is able to develop his or her talent to the full. We aim to promote in all members of our community, faith and religious commitment, in accordance with the rites, practices and teachings of the Catholic Church.

At Padre Pio we are proud to promote the United Nations Convention on the Rights of the Child and ensure that the whole school community learns about their rights and show respect for each other.

We have linked the following Rights to our Online Safety Policy:

- Article 16 – We have the right to privacy
- Article 19 – We have a right to be safe

### 1. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Padre Pio 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 digital technology on the school site (where allowed).**

Padre Pio Primary 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.

### 2. Vision and Rational

Padre Pio Catholic Primary School believes that Information and Communication Technology is an integral part of learning to prepare our pupils for today's society. It is imperative that we equip them with evaluative skills to use the internet safely in and out of school. Recognising Online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim". (Dr Tanya Byron, 2008)

## Policy and leadership

### Responsibilities

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

### Headteacher and senior leaders

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

### Governors

[Keeping Learners Safe](#) states:

2.38. “All governors, including the chair of governors, should be given access to safeguarding and child protection training to ensure a basic and consistent level of awareness. This training includes, but is not limited to, the Keeping learners safe modules.”

3.61. “The DSP should liaise with the designated governor for safeguarding so that the designated governor can report on safeguarding issues, irrespective of whether the issue is online or offline, to the governing body”

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 (*insert name of governor group/committee*) whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor<sup>2</sup>

to include:

---

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

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

## **Online Safety Lead**

In Padre Pio the online safety lead is currently the Designated Safeguarding Person (DSP)

The online safety lead will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with local authority technical staff
- meet regularly with the online safety/safeguarding governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to senior leadership team.
- liaises with the local authority/relevant body.

## **Curriculum Leads**

The [Keeping Learners Safe](#) safeguarding audit tool suggests:

“The curriculum should support existing policy within the education setting on important issues and provide sufficient information on managing risk, e.g. in: sex and relationships; drug, alcohol and tobacco education; accident prevention; anti-bullying; online safety; extremism and radicalisation.”

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme
- the Digital Competence Framework

- personal and social education/sex and relationships 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 for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [Live-streaming and video-conferencing: safeguarding principles and practice guidance](#).
  - [Keeping Learners Safe](#) (Paragraph 7.6) states: "Safeguarding is an integral principal of digital learning and the safety and welfare of learners must take precedence over all other considerations. Safeguarding must be integral to the delivery of live-streamed lessons to ensure learners are appropriately protected."
- 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.

## 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.

[Enhancing digital resilience in education: An action plan to protect children and young people online](#) (November 2022) states:

*“We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone’s business.”*

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
- *providing opportunities for parents and carers to improve their understanding of online safety through parents’/carers’ evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns and literature*

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

- *reinforcing the online safety messages provided to learners in school*
- *the use of their children’s personal devices in the school ([where this is allowed](#))*

## 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
- 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 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 and assemblies. Learner groups / classes are encouraged to suggest child friendly versions of the rules.
- staff /volunteer AUAs will be agreed and signed by staff and volunteers
- parent/carers 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 induction and handbook
- communication with parents/carers
- built into lessons
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul> <p>N.B. Schools should refer to guidance about dealing with self-generated images/sexting - <a href="#">guidance about dealing with nudes and semi-nudes being shared.</a></p>					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>• 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)</li> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul> <p>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – read more about this: <a href="#">NCA Cyber Choices Programme</a></p>					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

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

<p>Consideration should be given for the following activities when undertaken for non-educational purposes:</p> <p>Schools may wish to add further activities to this list.</p>	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/aware
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			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	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 the headteacher – 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 has in place procedures for identifying and reporting cases, or suspected cases, of online safeguarding issues/incidents and understands that because of our day-to-day contact with children our staff are well placed to observe the outward signs of these issues.

We ensure that every member of staff and every governor knows that they have an individual responsibility for reporting and that they are aware of the need to be alert to signs of abuse and neglect, and know how to respond to a learner who may disclose such issues.

We also understand that reporting systems do not always respond to the needs of learners and that we need to identify issues and intervene early to better protect learners.

*Schools should understand that online behaviours change, there is a risk that by drawing attention to certain behaviours, schools may inadvertently push children and young people towards the very content from which they are trying to protect them. Therefore, particular care should be given to the*

*manner in which information is shared by schools about online challenges and hoaxes. More information is available in this [guidance on Hwb](#).*

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 immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Person / Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same computer for the duration of the procedure.
  - it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (**except in the case of images of child sexual abuse – see above**).
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - internal response or discipline procedures

- involvement by local authority (as relevant)
  - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- 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 (as relevant and anonymously) to:
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school text messaging services, 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.



## 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: [\(the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column\(s\) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions\)](#)

## 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 <a href="#">in earlier section on User Actions</a> on unsuitable/inappropriate activities).		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	
Corrupting or destroying the data of other users.	x					x		x	x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x		x	x
Unauthorised downloading or uploading of files or use of file sharing.	x	x	x			x		x	
Using proxy sites or other means to subvert the school's filtering system.			x		x	x			
Accidentally accessing offensive or pornographic material and failing to report the incident.	x	x	x	x		x			

Deliberately accessing or trying to access offensive or pornographic material.	x	x	x		x	x		x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	x	x	x			x			
Unauthorised use of digital devices (including taking images)	x	x	x			x		x	x
Unauthorised use of online services	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	
Continued infringements of the above, following previous warnings or sanctions.			x			x	x		x

## Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)</b>		X	X	X				
Deliberate actions to breach data protection or network security rules.		X			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		X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X		
Unauthorised downloading or uploading of files or file sharing.		X			X	X		X
Breaching copyright or licensing regulations.		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X				X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		X				X		
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X				X		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail.		X				X		X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner.		X			X	X		
Actions which could compromise the staff member's professional standing.		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
Failing to report incidents whether caused by deliberate or accidental actions.		X				X		X
Continued infringements of the above, following previous warnings or sanctions.		X			X	X	X	X

## Education

### Online Safety Education Programme

Enhancing digital resilience in education: An action plan to protect children and young people online states:

“With so many aspects of our lives now entwined with using technology in an online world, supporting our children and young people to be digitally resilient is fundamental. Digital resilience encapsulates the need to develop knowledge, skills and strategies in order for children and young people to:

- manage their online experience safely and responsibly while protecting their digital identity
- identify and mitigate risks to stay safe from harm online
- understand the importance of using reliable sources and employing critical thinking skills to identify misinformation
- seek help when they need it
- learn from their experiences and recover when things go wrong
- thrive and benefit from the opportunities the internet offers.”

“Building digital resilience within our children and young people prepares them to become well-rounded and balanced citizens that recognise the impact of their actions. Ensuring our children and young people use technology responsibly to foster a culture where mental and physical health is not adversely affected by the internet is crucial.

Supporting the social and cultural development of our children and young people, including promoting values such as tolerance and respect for others in all environments, is another overarching objective, which we set out to achieve through our online safety education activities.”

Guidance for education settings on peer sexual abuse, exploitation and harmful sexual behaviour states:

“Young people increasingly experience abuse and exploitation online and/or digitally. This will be more difficult for education settings to identify, as some of it is likely to occur outside schools and colleges. However, it is important to consider the impact of this on young people’s offline lives.”

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/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, SEND 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. [NB additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires 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*
- the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

## Contribution of Learners

[Keeping Learners Safe](#) states:

“How safe do learners feel? The United Nations Convention on the Rights of the Child (UNCRC) sets out that children have a right to be safe and protected from harm, and have the right to express their opinions and participate in decision-making. In accordance with the UNCRC, the best way to understand how safe an education setting feels to learners is to ask them and observe how they and staff interact.”

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:

- *pupil questionnaires and surveys*
- *appointment of digital leaders*
- *learners contribute to the online safety education programme e.g. digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

## **Staff/volunteers**

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

- **a planned programme of formal online safety, cyber security 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.** *It is expected that some staff will identify online safety as a training need within the performance management process*
- **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 / Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

## **Governors**

**Governors should take part in online safety training/awareness sessions**, 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 ([this may include attendance at assemblies/lessons](#)).

## **Families**

[Enhancing digital resilience in education: An action plan to protect children and young people online](#) states:

*“Building digital resilience in our children and young people also depends on the resilience of our families and communities. We are committed to nurturing and promoting the safe and positive use*

of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business."

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, 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](#)*
- *Sharing good practice with other schools in clusters and or the local authority*

## **Adults and Agencies**

The [Enhancing digital resilience in education: An action plan to protect children and young people online](#) draws upon the self-review information schools in Wales record in the 360 safe Cymru tool. This data highlights that schools showing the strongest performance, amongst other indicators,

*'ensure that parents and carers receive these important online safety messages, often through the learners themselves sharing the messages learned in school. The school will also share their good practice with the wider community and other schools and will make use of the valuable community resources available to them from agencies such as the police'.*

Drawing on this intelligence, 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:

- providing family learning courses in use of new digital technologies and online safety
- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their learning platform, website, and social media for the wider community

The school recognises the support and advice that may be provided by external groups and agencies and values their contribution to school programmes and events.

## Technology

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

[Keeping Learners Safe](#) states:

7.7. "It is critical that web-filtering standards are fit for purpose for twenty-first century learning and teaching, allowing the access schools require while still safeguarding children and young people. Governing bodies should ensure appropriate filters and appropriate monitoring systems are in place and refer to web filtering standards as part of the Education Digital Standards for schools in Wales. The standards seek to support schools to provide a safe, responsible and supportive environment to learn in, and prevent access to inappropriate or harmful content. Responding to incidents of sharing nude or semi-nude images"

## Filtering

- the school filtering policies are controlled by SRS and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government [Recommended web filtering standards for schools](#) and the UK Safer Internet Centre [Appropriate filtering](#).
- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- *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

If necessary, the school will seek advice from, and report issues to, SRS and LA

## Monitoring

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through:

- physical monitoring (adult supervision in the classroom)
- 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.*

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

## Mobile technologies

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device <sup>3</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes		No	No
Internet only					Yes	Yes

## Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online. The [practitioner's guide to using social media](#) on Hwb provides further information.

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

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

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

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

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

### **Personal use**

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

### **Monitoring of public social media**

- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

### **Digital and video images**

The 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. It is common for employers to carry out internet searches for information about potential and existing employees.

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](#) para 7.6**
- **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. The personal equipment of staff should not be used for such purposes
- care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. ([see parents and carers acceptable use agreement in the Appendix](#)). [Permission is not required for images taken solely for internal purposes](#)
- 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
- Online newsletters
- Other

The school website is managed/hosted by [\(insert details\)](#). 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.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process*

## Data Protection

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

The school:

- **has a Data Protection Policy. [\(see appendix for template policy\)](#)**
- **implements the data protection principles and is able to demonstrate that it does so**
- **has paid the appropriate fee to the Information Commissioner's Office (ICO)**
- **has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. [The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO](#)**
- **has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed**
- **has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it**
- **information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this**



- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject, **e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them**
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers. **In Wales, schools should consider using the [Wales Accord on Sharing Personal Information](#) toolkit to support regular data sharing between data controllers**
- has clear and understood policies and routines for the deletion and disposal of data
- **[reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents**
- **As a maintained school**, has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- no personal data should be stored on any removable media

**Staff must ensure that they:**

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school

- **will not transfer any school personal data to personal devices.** [Procedures should be in place to enable staff to work from home \(i.e. VPN access to the school network, or a work laptop provided\).](#)
- **use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data**
- **transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.**

## Cyber Security

[Enhancing digital resilience in education: An action plan to protect children and young people online](#) describes cyber security as:

“The term used to describe how both individuals and organisations can reduce the risk of cyber attacks. Cyber security’s main purpose is to ensure the technology we use (devices such as computers, tablets and smartphones) and the services we access online are protected from the risk posed by cyber crime including theft for gain such as ransomware attacks and seeking competitive advantage, or malicious damage intended to disrupt an organisation’s ability to operate effectively. We store large amounts of personal and organisational information on devices and services and preventing unauthorised access to this information is critical.”

The [‘Cyber security in schools: questions for governing bodies and management committees’](#) guidance produced by the National Cyber Security Centre (NCSC) working with Welsh Government aims to support governing bodies’ and management committees’ understanding of their education settings’ cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the school has adopted and made use of the relevant Hwb [Network and Data Standards](#)
- the school, in partnership with their education technology support partner, has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school, in partnership with their education technology support partner (SRS), has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security
- staff receive training on the common cyber security threats and incidents that schools experience

- the school has a business continuity and incident management plan in place that includes IT and these wider services.

## Outcomes

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

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

## Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be [downloaded from Hwb](#).

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

### Acknowledgements:

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

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use. Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in March 2023. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2023

## Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. To protect personal data we will

ensure that we take account of policies and guidance provided by the local authority and other relevant bodies. **(Further information and guidance is included in appendix B.)**

### **The Protection of Personal Data**

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The

Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **1. POLICY DECISIONS**

### **Authorising Access to the Internet.**

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

### **Progression Step 1 and 2 (Reception – Year 2)**

Access to the Internet will be by adult demonstration and directly supervised access to specific, approved online materials.

### **Progression Step 2 and 3 ( Years 3 – 6)**

Pupils should be able to access the internet independently under supervision by a member of staff.

Pupils and parents should discuss and agree and sign the Acceptable Use Policy and have a clear understanding of online safety rules for Padre Pio Catholic Primary School.

Parents will be asked to sign and return a consent form for pupil access.

Parents will be informed that pupils will be provided with supervised Internet access.

### **Risk Assessment**

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor

Torfaen County Borough Council can accept liability for the material accessed, or any consequences resulting from Internet use

Padre Pio Catholic Primary School will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

### **Handling Online safety Complaints**

Complaints of internet misuse will be dealt with under our School's Complaints Procedure.

Any complaint about staff misuse must be referred to the Head Teacher.

All online safety complaints and incidents will be recorded by the school — including any actions taken.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will work in partnership with staff to resolve issues.

Discussions will be held with the local Police Community Support Officer and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

### **The Internet in the Community**

The school will liaise with local organisations to establish a common approach to online safety.

The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

All members of the community who use internet facilities within the school will complete an appropriate Acceptable Use Policy.

### **Responding to incidents of misuse**

#### **Illegal Incidents**

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

### **Managing Cyberbullying and Cyber Incidents**

Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. There are clear procedures in place to support anyone affected by Cyber bullying as set out in Padre Pio Catholic Primary School's Anti-Bullying Policy.

All incidents of cyber bullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of cyber bullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Pupils, staff and parents/carers will be advised to not delete the offending texts, emails, video etc.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in cyber bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

## **COMMUNICATION POLICY**

### **Pupils**

All users will be informed that the network and internet will be monitored. Pupils sign an acceptable user agreement [Appendix 2] to show that they understand the systems in place. This is acknowledged by parents.

A programme of online safety awareness activities will take place regularly in all year groups throughout the school year to raise the awareness and importance of safe and responsible internet access. Pupil instruction in responsible and safe use will precede Internet access.

Safe and responsible use of the internet and technology will be reinforced across the curriculum, including PSE and citizenship covering both home and school access. Particular attention will be given where pupils are considered to be vulnerable.

### **Parents.**

Online safety requirements and information (acceptable use agreements and digital consent agreements) are included in the induction process for new pupils and parents.

### **Enlisting Parents' Support**

Parents' and carers' attention is drawn to the school online safety policy via the school prospectus and on the school website, and parent workshops will also be used when appropriate.

Parent/Carer and pupil surveys will be used to help identify any weaknesses and/or strengths with regard to our online safety practice/policy.

Parents are asked to sign a Parent/Carer Acceptable use of ICT agreement [Appendix 4] to show understanding that making critical, derogatory or malicious comments about the school on social networking sites (i.e. Facebook, Twitter) is unacceptable and may result in legal action.

## Appendices – Section A - Acceptable Use Agreement

- A1 Pupil Acceptable Use Agreement (younger children)
- A2 Pupil Acceptable Use Agreement (older children)
- A3 Staff and Volunteers Acceptable Use Agreement
- A4 Parents / Carers Acceptable Use Agreement
- A5 Responding to incidents of misuse – flow chart
- A6 Reporting Log

### Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	P & I Committee 1/5/2024 Full Governors 22 May
The implementation of this Online Safety Policy will be monitored by:	SLT and Governors' P & I Committee
Monitoring will take place at regular intervals:	Annually
The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA safeguarding officer, police etc

### Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

1. logs of reported incidents
2. surveys/questionnaires of:
  - learners
  - parents and carers
  - staff.

## **A1 Pupil Acceptable Use Policy Agreement – for younger pupils (PS1 and Lower PS2)**

**This is how we stay safe when we use computers:**

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

*Signed (child):.....*

*(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)*

Signed (parent): .....



## A2 Pupil Acceptable Use Agreement – Upper PS2 and PS3

### Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

### This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and the internet, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

## Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

### For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of “stranger danger” when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

### I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

### I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I am not allowed to use my mobile phone in the school. If I have permission to bring my phone to school, it must be handed in to the office every day.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may not be allowed to use devices and parents will be contacted.

### Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

## A3 Staff (and Volunteer) Acceptable Use Policy Agreement

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

#### This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online safety in my work with young people.

#### For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

#### I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)

- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any Online activity that may compromise my professional responsibilities.

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :**

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools / academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

## A4 Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online safety and are involved in the education and guidance of young people with regard to their Online behaviour.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

### Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

*I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

Or: (KS1)

*I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

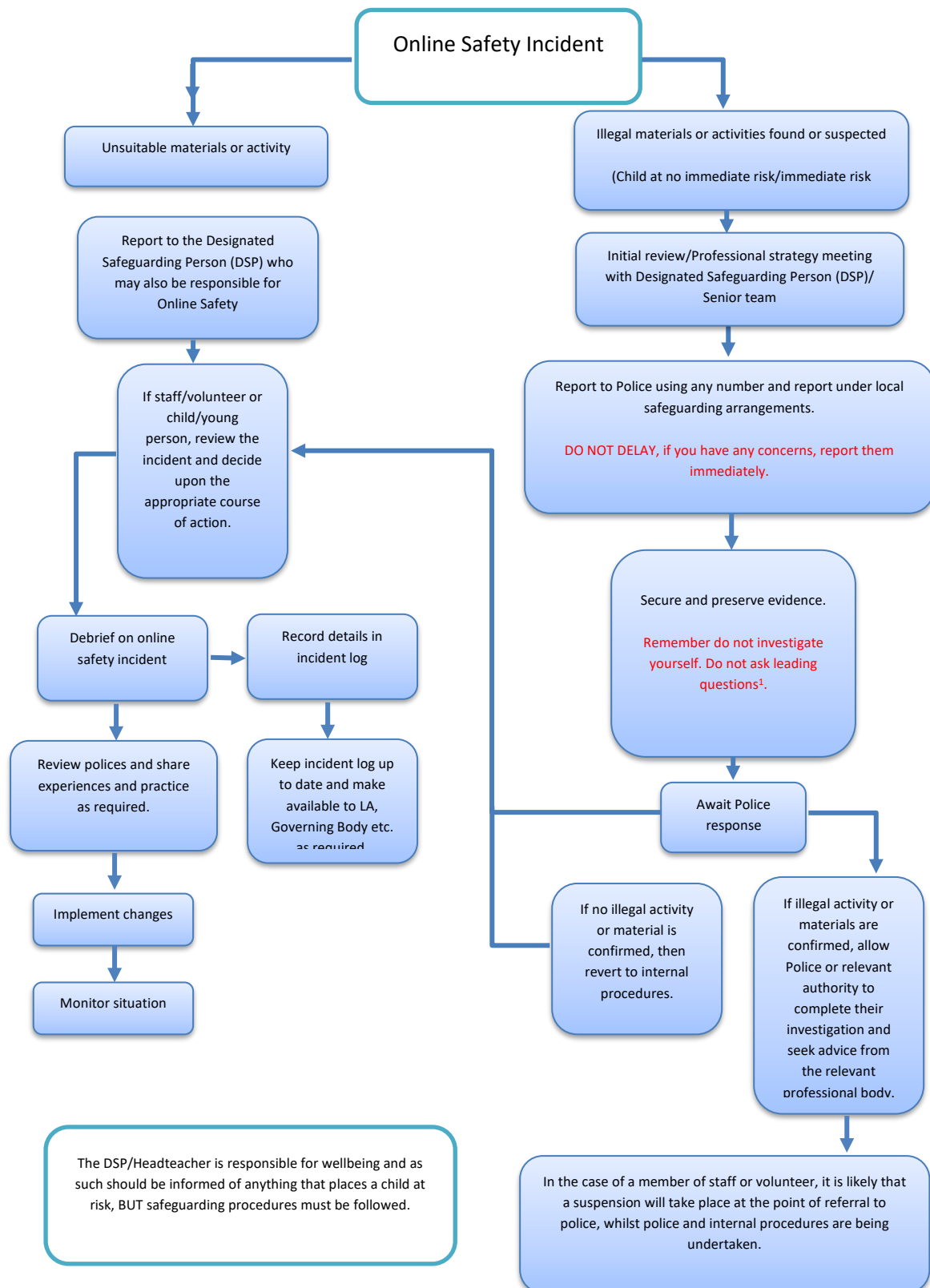
I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online safety.

Signed

Date

## A5 Responding to incidents of misuse – flow chart



**A6 Reporting Log** School: .....

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