

Our Lady of Peace Catholic Primary and Nursery School



Online Safety Procedure

By order of the Governing Body of Our Lady of Peace Primary School and Nursery

Review Dates:	Date Reviewed: FGB 19/05/2022	Next Review: May 2024
----------------------	--------------------------------------	------------------------------

Scope of the policy

This policy applies to all members of the school community (including pupils, staff, governors, parents/carers, volunteers, PTA) who have access to and are users of school ICT systems, both in and out of the school. It also applies to members of the school who access the internet and social media away from the school's premises.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

School Online Safety Officer: Mr N. Stopps, Assistant Headteacher

Designated Safeguarding Lead: Mrs Helen Hadaway

Designated Safeguarding Governor: Mrs K Slattery

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs

- reporting to relevant Governors committee meetings

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- 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 (see flow chart on dealing with online safety incidents).
- The Headteacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Officer

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings of Governors.
- Reports regularly to the Senior Leadership Team.

Network Manager/Technical Staff:

The Computing Leader is responsible for liaising with the technical team to ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any Local Authority, DFE or Ofsted Online Safety Policy/Guidance that may apply.
- That user may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- That the use of the network/internet/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Officer for investigation/action/sanction.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the Online Safety Officer for investigation/action/sanction.
- All digital communications with pupils/parents/carers should only 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.
- They 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 pupils 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.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / 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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Officer with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Students/Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- 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 or cyber-bullying.
- 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/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evening, newsletters, letters, website/Learning Platform and information about national online safety campaigns. Parent and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/Learning Platform.
- Their children's personal devices in the school.

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety is therefore an essential part of the school's online safety provision. Children and

young people need the help and support of the school to recognise and avoid online safety risks and build 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils 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. Under the Counter Terrorism and Securities Act 2015 schools are required to ensure that children are safe from terrorist and extremist material on the internet.
- pupils should be helped to understand the need for the pupil 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 pupils 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 students / pupils are allowed to freely search the internet, staff should be vigilant in 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 (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove 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.

Education – Parents/Carers

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 on-line 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 therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> (see appendix for further links / resources)

Education – The Wider Community

The school will provide opportunities for local community groups / members of the 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, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

Education & Training – 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 training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should 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 is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events (eg from 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 / phase meetings / INSET days.
- The Online Safety Officer will provide advice / guidance / training to individuals as required.

Training - Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure/equipment, filtering and monitoring

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 online safety responsibilities:

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 must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by TSI (Technical Support) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (6 Months).
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg locked cupboards in Business Managers office)
 - The Business Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Guidance is in place (Visitors Pack) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (Staff Acceptable Use Agreement) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (Staff Acceptable Use Agreement) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See School Personal Data Guidance in the appendix for further detail)

Mobile Technologies (Including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: Laptop, tablet or other technology that usually has the capability of utilizing the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the usage and appropriate use of mobile technologies should be an integral part of the school’s Online safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.
- The school allows:

	School Devices		Personal Devices		
	School Owned for single user	School Owned for multiple users	Student Owned	Staff Owned	Visitor Owned
Allowed in school	Yes	Yes	No	No	Yes ¹
Full network access	Yes	Yes	No	No	No
Internet Only	Yes	Yes	No	No	Yes
Network access	Yes	Yes	No	No	No

A visitor to the school will be allowed (with prior permission from SLT) to bring in a personal device and have access to the internet if it will support the education of the pupils. (e.g. Slough Music Service – to deliver music lessons in Year 5)

School Owned/provide devices:

- Devices will be allocated to staff members only
- Laptops and tablets can be used in and outside of school
- School owned/provided devices should not be used for personal use
- All school owned/provided devices will have full access to the network and internet
- Devices will be managed by the computing leader and technical support team. Staff should not install software/apps onto any school owned/provided device
- Devices will use the schools filtering system
- When staff members leave, all school owned/provided devices should be handed back to the computing leader. Technical support team will then clean and prepare the devices for the next member of staff
- Staff training shall be provided to staff in how to use the devices
- As described in the ‘Staff Acceptable Use Agreement’, Staff will be liable for any damage caused to school devices outside of school.

Personal Devices

- No personal devices should be brought and utilized in the school for educational or communication purposes
- Visitors can bring in devices and have access to the internet only with prior permission from SLT. The purpose is to support the teaching of lessons (e.g. Slough Music Service)

Smart Watches

Pupils are not permitted to wear Smart Watches or other similar style watches for safeguarding reasons. These are not suitable for wearing in school for a number of reasons. Many of these watches have internet connection which if used within school could pose a safeguarding risk. They are also costly items, which could easily be damaged or go missing and can be a distraction in class.

Children may wear a simple analogue or digital watch to enable them to tell the time.

If these watches have alarms, they should be switched off during school times. If a watch is deemed to cause distraction within the classroom, it will be removed and a parent required to collect it from the school office.

We are aware that some children are wearing fitness trackers/fitbits at home in order to develop their healthy lifestyles and monitor their exercise throughout the day. Previously these have caused a distraction when brought into school and governors have, therefore, decided that these may not be brought into school or worn during the school day. In exceptional circumstances the Headteacher may choose to authorise these being worn.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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:

- When using digital images, staff should inform and educate pupils 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/local press
- 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner’s Office.

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.
- 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 and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected

- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults				Students				
	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission and supervision	Not Allowed
Mobile phones may be brought to the school		✓				✓			
Use of mobile phones in lessons	✓				✓				
Use of mobile phones in social times		✓			✓				
Taking photos on mobile phones	✓				✓				
Use of other mobile devices e.g. tablets		✓			✓				
Smart watches, fitness trackers/fitbits can be brought into school		✓			✓				
Use of Smart Watches, fitness trackers/fitbits in social times		✓			✓				
Use of Smart watches, fitness trackers/fitbits in lessons	✓				✓				
Use of personal email addresses in school, or on school network			✓		✓				

Use of school email for personal emails	✓				✓				
Use of messaging apps	✓				✓				
Use of social media	✓				✓				
Use of blogs			✓					✓	

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

- The official school email service (Staff: Office 365, Pupils: ESchools) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to the Online Safety Officer – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at EYFS, KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils 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, cyberbully, 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, 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

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies.

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

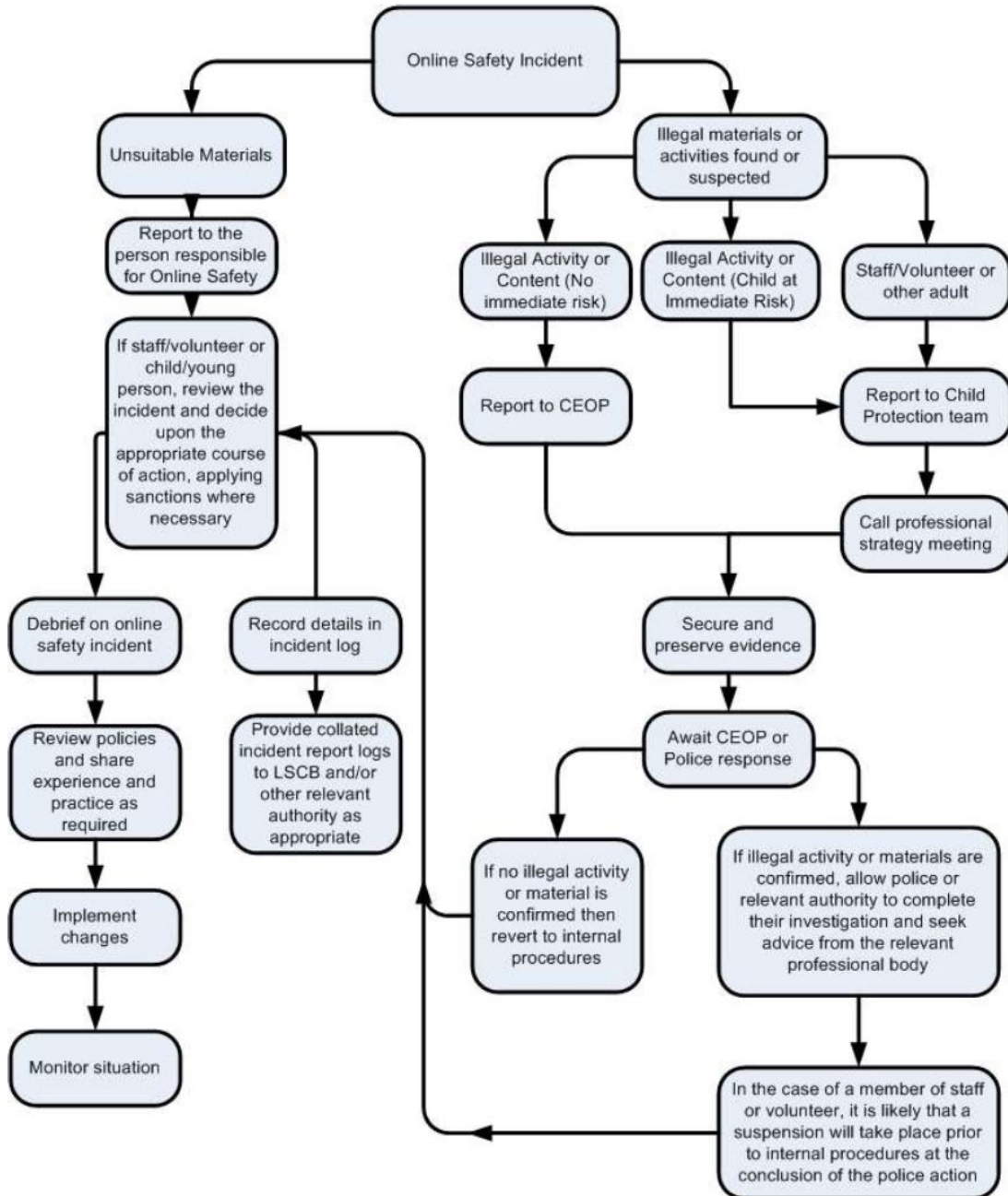
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
	Creating or propagating computer viruses or other harmful files				X	
	Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
	On-line gaming (educational)			X		
	On-line gaming (non-educational)				X	
	On-line gambling				X	
	On-line shopping / commerce				X	
	File sharing			X		
	Use of social media				X	
	Use of messaging apps				X	
	Use of video broadcasting e.g. Youtube				X	

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer 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 young people and if necessary can be taken off site by the police should the need arise. 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 below)
- 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 or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police 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
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

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:

	Actions/Sanctions								
	Refer to class teacher	Refer to Assistant Headteacher	Refer to Deputy Head/Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Pupils Incidents									
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓					✓		✓	
Unauthorised / inappropriate use of mobile phone/digital camera / other mobile device	✓	✓				✓		✓	

Unauthorised / inappropriate use of social media/messaging apps / personal email	✓	✓				✓		✓	
Unauthorised downloading or uploading of files	✓				✓			✓	
Allowing others to access school network by sharing username and passwords		✓	✓		✓				✓
Attempting to access or accessing the school network, using another pupils account.		✓	✓		✓		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓		✓		✓		✓
Corrupting or destroying the data of other users		✓	✓		✓		✓		✓
Pupils Incidents (Continued)	Actions/Sanctions								
	Refer to class teacher	Refer to Assistant Headteacher	Refer to Deputy Head/Headteacher	Refer to Police	Refer to technical support staff for action re	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g. detention/exclusion
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓						✓
Continued infringements of the above, following previous warnings or sanctions			✓						✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓						✓
Using proxy sites or other means to subvert the school's filtering system			✓		✓		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓				✓
Deliberately accessing or trying to access offensive or pornographic material			✓		✓		✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓						✓

Staff Incidents	Actions/Sanctions
-----------------	-------------------

	Refer to Assistant Headteacher	Refer to Deputy/Headteacher	Refer to Local Authority	Refer to Police	Refer to technical support staff for action re	Inform parents/carers	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)		✓	✓	✓					✓
Inappropriate personal use of the internet/social media/personal email.		✓					✓		
Unauthorised downloading or uploading of files	✓						✓		
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.	✓	✓					✓		
Staff Incidents	Actions/Sanctions								
	Refer to Assistant Headteacher	Refer to Deputy/Headteacher	Refer to Local Authority	Refer to Police	Refer to technical support staff for action re	Inform parents/carers	Warning	Suspension	Disciplinary Action
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓	✓	✓				✓	✓
Deliberate actions to breach data protection or network security rules		✓	✓	✓				✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓				✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓			✓	✓	✓
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils		✓	✓	✓				✓	✓
Actions which could compromise the staff member's professional standing		✓	✓	✓			✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓	✓				✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓	✓	✓			✓	✓

Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	✓			✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				✓	✓
Breaching copyright or licensing regulations		✓	✓	✓				✓	✓
Continued infringements of the above, following previous warning or sanctions		✓	✓	✓				✓	✓

Appendices







Pupil and Parent Acceptable Use Agreement EYFS and KS1	24
Pupil and Parent Acceptable Use Agreement KS2	25
Using images of children consent form	26
Staff Acceptable Use Agreement	28
Responding to incidents of misuse – flow chart	30
Record of reviewing devices/internet sites (Responding to incidents of misuse)	31
Online Safety Incident Form	32
School Personal Data Handling Guidance	33
Staff help sheet for assessing risk of sharing information	40
Template for a register of sensitive data held by the school	42
Timetable for information security management	43



Our Lady of Peace Catholic Primary and Nursery School

'With Christ in our hearts together we grow'

EYFS & KS1 Pupil and Parent Acceptable Use Policy

Think then Click E-Safety Rules for EYFS and Key Stage 1		
These rules help us to stay safe on the Internet		
	We only use the internet when an adult is with us	
	We can click on the buttons or links when we know what they do.	
	We can search the Internet with an adult.	
	We always ask if we get lost on the Internet.	
	We can send and open emails together.	
	We can write polite and friendly emails to people that we know.	



At Our Lady of Peace all pupils use computer facilities including internet access as an essential part of learning. Parents/Carers are asked to sign below on behalf of their child to show that the Online Safety rules have been understood and agreed. Parents/Carers will support the school to encourage their child to always use technology in a safe way.

Online Safety Agreement

- I have read and understood the School Online Safety rules.
- I will use the computers, school network, internet access, Learning Platform and other new technologies in a sensible way.
- I know that the school network and internet access are monitored.

Pupil Name: _____

Parent/Carer Signature: _____

Parent Carer Name: _____



Our Lady of Peace Catholic Primary and Nursery School

'With Christ in our hearts together we grow'

KS2 Pupil and Parent Acceptable Use Policy

Think then Click

Online Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.



At Our Lady of Peace all pupils use computer facilities including internet access as an essential part of learning. Both pupils and their parents/carers are asked to sign below to show that the online safety rules have been understood and agreed.

Online Safety Agreement

- I have read and understood the School Online Safety rules.
- I will use the computers, school network, internet access, learning platform, and other new technologies in a sensible way.
- I know that the school devices, network and internet access are monitored.

Pupil Signature: _____

Pupil Name: _____

Parent/Carer Signature: _____

Parent/Carer Name: _____



Our Lady of Peace Catholic Primary and Nursery School

'With Christ in our hearts together we grow'

USING IMAGES OF CHILDREN CONSENT FORM

Child's Name -----

Occasionally we take photographs of the children at our school. We may use these images on our school website or in other printed publications. We may also make video or webcam recordings for parents' information meetings, school-to-school conferences, monitoring or other educational use.

Photographs or film footage by parents or guardians of their children at school events is permitted under an exemption in the Data Protection Act 1998. There is also a journalistic exemption with regard to the media and occasionally pupil's images may appear in local or national newspapers, or on televised news programmes. If you do not wish your child to appear in the media, we will try to keep your child out of the photographs.

We need your permission before we can photograph or make any recordings of your child, in order to comply with the Data Protection Act 1998.

Please can you complete the form below and return to the school office.

Please circle your answer

- | | |
|--|----------|
| 1. May we use your child's photograph in printed publications? | Yes / No |
| 2. May we use your child's image on our website? | Yes / No |
| 3. May we record your child's image on video or webcam? | Yes / No |
| 4. Are you happy for your child to appear in the media? | Yes / No |

I have read and understood the Condition of use overleaf.

Parent/Guardian signature -----Date-----

Conditions of use: -

1. This form is valid from the date you sign, for the period of time your child attends this school. The consent will automatically expire after this time.
2. We will not use the personal details or full names of any child in a photographic image on video, on our website, or in any of our printed publications.
3. We will not include personal email or postal address or telephone or fax numbers on video, on our website, or in other printed publications.
4. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.
5. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.
6. We may include pictures of pupils and teachers that have been drawn by pupils.
7. We may use group or class photographs or footage with very general labels, such as “a science lesson” or making “Christmas decorations”.
8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

Pictures/Recordings

Taking pictures or recordings of your own children for your own personal use is permitted under the Data Protection Act. The difficulty arises with plays or other events in that other children may also be filmed. It is important that we are all aware that some members of the community (children or adults) may be vulnerable and must not have their image shared online as they could be put at risk from harm. You may not always know who these people are and we need everyone’s support to protect the whole community. It is also important for us all to role model positive behaviour for children, so check first before posting any images online which contain other children than your own. If you do NOT have permission please do not put any photos or videos on any social networks. Parents/Carers should not copy images from the school/ setting site without appropriate permission from the school/setting.

I have read, understood and accept the above statement on Pictures/Recordings

Name:

Signed:

Date:



Our Lady of Peace Catholic Primary and Nursery School

'With Christ in our hearts together we grow'

Staff Acceptable Use Agreement

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, virtual learning environment, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure email system for school business (currently Office 365 mail).
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Computing Leader and Online Safety Officer.
- I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed. If I am unsure I will seek advice from the Computing Leader or Technical Support Team.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my line manager, the Computing Leader or the Head Teacher on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, laptop or other device (including USB flash drive), to a network or Internet that does not have up-to-date anti-virus software. If I believe that the anti-virus is not up to date I will immediately inform the ICT Technical Support Team.
- I will not use personal digital cameras or camera phones for taking images of pupils or staff other than in accordance with the school's digital image/photographic policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites, blogs etc that I create or actively contribute to are not confused with my professional role.
- I will not use the school's name or the names of children in online posts on social networking sites such as 'Facebook' or 'twitter'.
- I will not use the names of staff in online posts on social networking sites such as 'Facebook' or 'twitter' without permission.
- I will not use school computers to access Facebook, Twitter or any other social networking sites.
- I will ensure settings (on personal/home devices) are set to the highest setting on any personal social networking profiles.
- I will not post anything onto social networking sites that would offend any other member of staff or parents.

- I will not post photographs related to the school on any internet sites including photographs of or photographs containing school children, colleagues, parents or the school's uniform.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will ensure that laptops on loaned to me by the school are carried safely in their carry case to avoid damage.
- I will ensure that any laptop or equipment loaned to me by the school is not left unattended in any vehicle. I understand that I am liable for any damage to school property outside of school.
- I will not allow anyone else to use the school laptop when taking it off site.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority or for Child Protection.
- I will ensure I am aware of online safety-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that failure to comply with the Acceptable Use Agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Agreement.

I agree to abide by the school's most recent Acceptable Use Agreement.

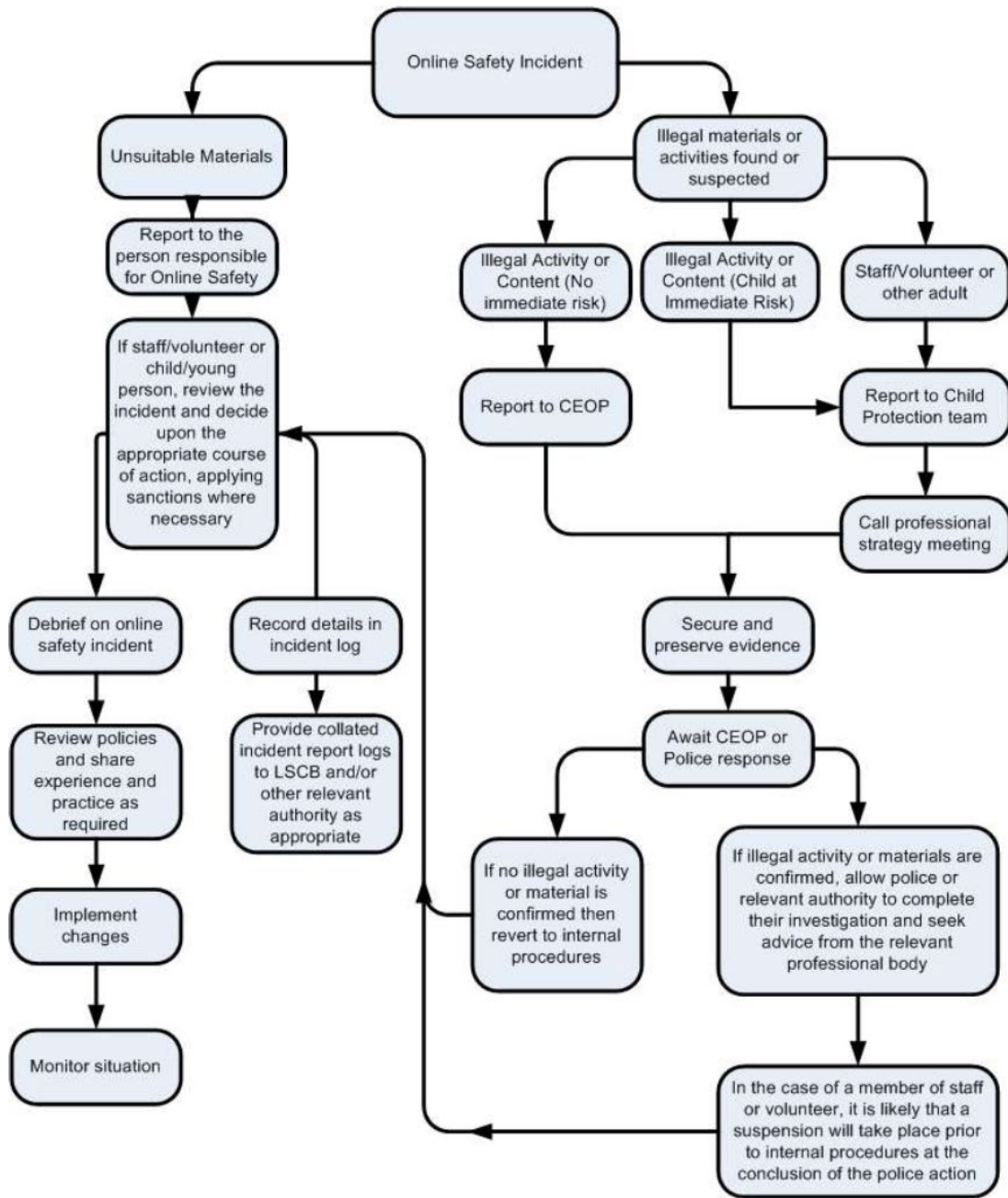
Signature Date

Full Name(printed)

Job title

School

Responding to incidents of misuse – flow chart





Our Lady of Peace Catholic Primary and Nursery School
'With Christ in our hearts together we grow'

Record of reviewing devices/internet sites
(Responding to incidents of misuse)

Group:

.....

Date:

.....

Reason for investigation:

.....
.....
.....
.....
.....

Details of first reviewing person

Name:

.....

Position:

.....

Signature:

.....

Details of second reviewing person

Name:

.....

Position:

.....

Signature:

.....

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

.....
.....
.....
.....



Our Lady of Peace Catholic Primary and Nursery School
'With Christ in our hearts together we grow'

Online Safety Incident Form

Date:	Time:
<u>Section A: Pupil Details</u>	
Surname:	Forename:
Male:	Female:
<u>Section B: About the Incident</u>	
What was the incident?	
Where did it take place?	
When did it take place?	
What action has been taken:	
What staff were involved:	
Was parent/class teacher informed:	
<u>Section C: The Person completing the report</u>	
Name/s:	
Signature:	
Countersigned by:	

Appendix

SECURE DATA HANDLING POLICY

Introduction

It is the responsibility of the school to register as a Data Controller on the Data Protection Register held by the Information Commissioner. The school has a data protection officer who will keep the school up-to-date with current legislation and guidance.

It is important to stress that this secure data handling policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- Have permission to access that data.
- Need to have access to that data.

Any loss of personal data can have serious effects for the individuals and/or institutions concerned. It can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution.

All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in current relevant data legislation and regulations. The loss of personal data by organisations and individuals over the last few years has made this a relevant and high-profile issue for schools and all organisations. It is important that the school has a clear and well understood personal data policy because:

- No school or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are 'data rich' and the introduction of electronic storage and transmission of data has created additional potential for the loss of data.
- The school will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations.

Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008 regarding Data Handling Procedures in Government. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that these procedures are adopted.

The school and individuals working in the school will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This can include:

- Personal information about members of the school community – including pupils/students, members of staff, parents and carers, eg names, addresses, contact details, legal guardianship, health records, disciplinary records.
- Curricular/academic data, eg class lists, pupil/student progress records, reports, references.
- Professional records, eg employment history, taxation and national insurance records, appraisal records and references.
- Information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Principles

As the role of management information systems (MIS) continues to develop, colleagues in schools have increasing access to a wide range of sensitive information.

There are generally two types of sensitive information:

- Personal data concerning the staff and pupils.
- Commercially sensitive financial data.

It is important to ensure that both types of information are managed in a secure way at all times. Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act as '*Data relating to a living individual who can be identified from the data*'.

The Act gives eight principles to bear in mind when dealing with such information. Data must:

- Be processed fairly and lawfully.
- Be collected for a specified purpose and not used for anything incompatible with that purpose.
- Be adequate, relevant and not excessive.

- Be accurate and up-to-date.
- Be processed in accordance with the rights of the data subject.
- Be kept securely.
- Not be kept longer than necessary.
- Not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

The Data Protection Act states that some types of personal information, defined as 'sensitive personal data' demand an even higher level of protection. This includes information relating to:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life (orientation).
- The commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

The three questions below can be used to quickly assess whether information needs to be treated securely:

- Would disclosure/loss place anyone at risk?
- Would disclosure/loss cause embarrassment to an individual or the school?
- Would disclosure/loss have legal or financial implications?

If the answer to any of the above is 'yes', then it will contain personal or commercially sensitive information and needs a level of protection.

Objectives and targets

The purpose of this policy is to advise all members of staff what is required by Our Lady of Peace Catholic Primary and Nursery School to ensure that it complies with the Data Protection Act at all times and to advise all members of staff how to proceed when handling data which needs to be handled securely.

Action plan

Procedures and practice

The following practices will be applied within Our Lady of Peace Catholic Primary and Nursery School:

- All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed.
- The amount of data held by the school will be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held by the school will be securely stored and sent by secure means.
- Every effort will be made to ensure that the data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.

Auditing

The school must be aware of *all* the sensitive data it holds, be it electronic or paper. Therefore:

- A register will be kept by the school data protection officer, detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated. Appendix 2 provides the template that will be used. This register will be checked by all team leaders each year to allow team members/colleagues to revise the list of types of data that they hold and manage.
- The length of time that individual sensitive documents need to be kept will be assessed using the Records Management Toolkit (See CEFM Management and retention of records policy).
- Audits will take place in line with the timetable for information security management. (See appendix 3). The audit will be completed by the data protection officer.

Risk assessment

The school will regularly carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available. The school's data protection officer is also the information risk officer, and s/he is responsible for the completion of the risk assessment. Carrying out a risk assessment will generally involve answering the following questions:

- How sensitive is the data?

- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

When these questions have been answered, the risk officer will be able to recognise the risks that are present, judge the level of those risks and prioritise them. Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

Appendix 1 offers a staff help sheet for assessing the risk of sharing information. Risk assessment will be an on-going process and the school will carry out assessments at regular intervals because risks change over time.

Securing and handling data held by the school

- The school will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on fixed station computers, laptops, portable devices and memory sticks.
- All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them. This will be the responsibility of the headteacher.
- The school has a clear policy and a procedure for the use of cloud-based storage systems, and is aware that data held in remote cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with the controls put in place by service providers to protect the data. (See the DFE document 'Cloud software services and the Data Protection Act 2014.')
- Biometric data complies with the same data protection principles outlined on pages 3–4 above and also with the Protection of Freedoms Act 2012. We ensure that each parent of a child at the school is notified that we use their child's biometric data as a part of our automated biometric information system. Since September 2013, the written consent of the parents is obtained before the data are taken from all pupils under 18 years of age. We will not process this data if the child under 18 (if deemed competent to understand the issue) refuses or if no parents or only one of two parents have consented in writing. The school provides alternative means of accessing services for those pupils who will not be using an automatic biometric recognition service.
- Staff should *not* copy or remove sensitive data from the school or authorised premises unless the media are:
 - Encrypted.
 - Transported securely.
 - Stored in a secure location.

- Sensitive data *should not* be transmitted in unsecured emails (eg pupil names and addresses, performance reviews etc).
- Data transfer should be through secure websites. If this is not available, then the file must be minimally password protected or preferably encrypted before sending via email. The password must be sent by other means, and on no account included in the same email. A record of the email should be kept to identify when, and to whom, the email was sent. (The DFE website contains a useful section – ‘*Transferring personal data securely between schools, LAs and the Department*’ (updated March 2014). This provides comprehensive guidance on transferring information.)
<http://media.education.gov.uk/assets/files/pdf/s/secure%20methods%20for%20transferring%20data.pdf>.
- Data (pupil records, SEN data, contact details, assessment information) must be automatically backed up, encrypted and stored in a secure place – eg safe/fire safe/remote backup facility.
- All staff computers, including laptops, must be used in accordance with the policy for ICT and use of the internet and intranet by staff.
- When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by the school’s ICT technical support staff.
- The school’s wireless network (wifi) will be secure at all times.
- Devices that are not the property of the school should only be used in line with our ‘Use of personally owned devices by staff policy’.
- The school will identify which members of staff are responsible for data protection, (also known as information asset owners). The line manager is the data protection officer.
- The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc know what data is held, who has access to it, how it is retained and disposed of. Appendix 2 details which members of staff are responsible for which data. This is shared with all staff concerned within the school.
- Where a member of the school has access to data remotely, the remote access off the school site to any personal data should be over an encrypted connection (eg VPN) protected by a username/ID and password. *This MIS information/school data must not be stored on a personal (home) computer.*
- Members of staff who are given full, unrestricted access to the school’s management information system must access the systems over an encrypted connection. *This MIS information/school data must not be stored on a personal (home) computer.*

- The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance and the records retention policy.

The school will securely delete commercially sensitive or personal data when it is no longer required according to the Records Management Society's guidance and the records retention policy.

The privacy notice

In order to comply with the fair processing requirements of the Data Protection Act, the school will inform parents and carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which this information is held and the third parties to whom it may be passed. Students deemed to be of a suitable age (usually 13+) are also made aware of the privacy notice, the school's legal obligations to pass on certain information (eg to providers of youth support services) and their rights to request the school to withhold certain information. Our privacy notice is worded according to the current DFE template and its circulation is supervised by our data protection officer.

Monitoring and reviewing

The policy will be monitored and evaluated regularly taking into account any incidents which occur, technological developments which might need a change in the policy or changes in legislation.

Staff help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, always take into consideration the nature of the information and the urgency of the situation, that is, take a risk-based approach to determining appropriate measures. The simplified process, described below will help members of staff and the school itself choose the appropriate level of security needed when sharing potentially sensitive information. The data protection officer is responsible for ensuring that staff are trained to use this process.

Step 1

Imagine a potential security breach (eg a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

- Will it affect or identify any member of the school or community?
- Will someone lose/be out of pocket by more than £100?
- Will it cause any kind of criminal case to fail?
- Is there a risk of discomfort/slur upon professional character of someone?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If the answer to all the above questions is 'no', the document does not contain sensitive information. If the answer is 'yes' to any of the questions above then the document will include some sensitive information and therefore requires a level of protection.

Step 2

Imagine the same potential security breach as above, and consider:

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Will an individual or someone who does business with the school lose/be out of pocket by £1,000 to £10,000?
- Will a serious criminal case or prosecution fail?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her professional reputation?
- Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If the answer to any of the above questions is 'yes' then the document contains sensitive information and additional security should be considered such as password protecting the document before you email it to a colleague outside of the school. However, if you think that the potential impact exceeds that stated in the question (eg someone's personal safety is at high risk) think very carefully before you release this information at all.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection/security if released at all. Err on the side of caution and seek guidance from the relevant line manager/senior member of staff.

Template for a register of sensitive data held by the school

Type of data	Held on	Period to be retained	Type of protection	Who can access the data

Timetable for information security management

Activity	Frequency	Lead
Audit of data held	Annually	Headteacher and admin officer
Encrypting sensitive data	On-going	All staff
Reviewing data backup procedures	Annual	Admin officer
Identifying staff responsible for data security and keep log of names and roles.	Annual	Headteacher
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT technical support
Wiping of laptop data when discarded	As necessary	ICT technical support