



St Mary's Primary School Draperstown

Online Safety Policy



Article 3

All adults should do what is best for you. When adults make decisions, they should think about how their decisions will affect children.

Co-Ordinator: Mrs Aileen Kearney

Mission Statement and Vision for ICT

At St. Mary's P.S. we aim to encourage the 'Learning Community' to be motivated by, gain confidence in and enjoyment from the use of ICT. We aim to be self-evaluative in the use of ICT, reflecting on current practice and keeping abreast of emerging technologies. St. Mary's Primary School strives to promote excellence in ICT through embracing new challenges to become competent, independent learners.

Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by:

- ICT Co-ordinator
- Staff - including Teachers and Support Staff
- Board of Governors
- Parents and Carers

Schedule for Development/Monitoring/Review

This Online Safety policy was updated approved by the Board of Governors on:	June 2021
The implementation of this Online Safety Policy will be monitored by the:	ICT Mrs A Kearney Principal Ms Coyle
Monitoring will take place on an on-going basis:	Mrs Kearney and Mr Bradley ICT Governor Link
The Board of Governors 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):	By Mrs Kearney annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	March 2021
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Education Authority Child Protection Team and the PSNI.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited /filtering).
- Internal monitoring data for network activity.
- Surveys/questionnaires of:
 - pupils
 - parents/carers
 - Staff

Scope of the Policy

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

The school will deal with online incidents within this policy and associated Positive Behaviour, Safeguarding 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

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

ICT	- Mrs A Kearney
Principal/DT	- Ms C Coyle
Vice-Principal/DDT/Numeracy Co-ordinator	- Mr G Brunton
Governor Link	- Mr P Bradley

Board of 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 Board of Governors, Mr P Bradley, has taken on the role of UICT and Online Safety Governor. The role of the Online Safety Governor:

- meetings with the Online Safety Co-ordinator
- attendance at Safeguarding meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors' meetings

Principal and Senior Leaders:

- The principal 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 UICT Co-ordinator, Mrs Kearney.
- The Principal and Vice-Principal will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents - included in a later section - "Responding to incidents of misuse.")
- The principal is responsible for ensuring that the UICT Co-ordinator and other relevant staff have access to suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Principal and Co-ordinator will ensure that there is a system in place to allow for monitoring.
- The Leadership Team and Board of Governors will receive regular monitoring reports from UICT Coordinator.

The Role of the UICT Coordinator

As the UICT Coordinator Mrs Kearney will;

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice for staff and organises training from outside agencies.
- Liaise with the Education Authority.
- Liaise with C2k technical support staff.
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meet regularly with UICT Governor, Mr Bradley to discuss current issues, review incident logs and filtering/change control logs.
- Attend relevant meetings/committees of Governors.
- Report regularly to the Leadership Team.
- Ensure that the school meets required online safety technical requirements and the Education Authority/DENI Online Safety Policy/C2k guidance that may apply.
- Ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are continually changed.
- Keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- Ensure 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 Principal/Vice-Principal/UICT Coordinator Safety Curriculum Leader for investigation.
- See that monitoring software/systems are implemented and updated.

Network Manager (C2K)

Mrs Kearney, Ms Coyle, Mrs O Kane, and Mr Brunton are C2k Managers.

The Network Manager (C2K) is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

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/Agreement (AUP).
- They report any suspected misuse or problem to the Principal/Vice-Principal; UICT Coordinator.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems, including the use of a private class 'Seesaw' group.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy and Acceptable Use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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 Teacher for Child Protection

Ms Coyle is the DT and Mr Brunton is the DDT. They are both trained in Online Safety issues and 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.

Safeguarding Team

Members of the Safeguarding Team include:

Margaret Heron, Chairperson of Board of Governors,

Karen Doyle, Board of Governors,

Ms Coyle, Principal and DT

Mr Brunton VP, DDT

Mrs Kearney ICT Co-ordinator/FS Co-ordinator

Mr Bradley, UICT Governor

The Safeguarding Team provides a consultative group that has representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy. The group will also be responsible for regular reporting to the Board of Governors.

Members of the Safeguarding Team will assist the ICT Curriculum Leader:

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

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good 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 the weekly Sway, Safer Schools App, information via Microsoft Teams and Seesaw, Information Sessions, letters, the school website, and information about national/local online safety campaigns/literature. Parents 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 and on-line pupil records.

Policy Statements

Education – Pupils

Article 29: *Your education should help you use and develop your talents and abilities. It should also help you learn to live peacefully, protect the environment and respect other people.*

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.

- A planned online safety curriculum will be provided as part of Computing and PDMU and should be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will 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.
- Pupils will 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 will 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 are 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 pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit. A member of staff will always be present when children have access to the internet.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that one of the C2k Managers or (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 apparent reasons for the need.

Education – Parents/Carers

The school will, therefore, seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Weekly Sway, Microsoft Teams and Seesaw, Twitter, Facebook, and the school website.
- Parents/Carers Information Sessions.
- High profile events/campaigns e.g., Safer Internet Day
- Reference to the relevant web sites/publications eg swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

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:

- 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.
- Regular posts on Twitter and Facebook

Education and 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 by the UICT Coordinator.
- All new staff should receive online safety training from the UICT Co-ordinator as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- Staff will have opportunities to identify online safety as a training need within the performance management process.
- The UICT Co-ordinator will receive regular updates through attendance at external training events 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 meetings/School Development Days.
- The UICT Co-ordinator will provide advice/guidance/training to individuals as required.

Training – Board of 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 will be offered through:

- Attendance at training provided by the Education Authority or other relevant organisation.

- Participation in school training/information sessions for Governors, staff, or parents (this may include attendance at assemblies).

Technical – Infrastructure/Equipment, Filtering and Monitoring

The Principal, VP and ICT Co-ordinator will be responsible for ensuring that the school infrastructure/network is as safe and secure as is possible and that policies and procedures approved within this policy are implemented.

- 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 will be provided with a username and secure password by Mrs Kearney/ Mrs O'Kane 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 regularly. Individual PINs are used for Foundation Stage.
- The passwords for the school ICT system, used by the Mrs Kearney/ Mrs O'Kane must also be available to the principal and kept in a secure place.
- Mrs Kearney is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by C2K. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes – these must be written into the ICT book and agreed by the Online Safety Team.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-levels at each Key Stage filtering (allowing different filtering levels for different ages/stages and distinct groups of users – staff/ pupils).
- 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.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts

which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date virus software.

- An agreed policy is in place for the provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that 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.**
(Refer to Data Protection Policy)

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop, or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school'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 mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Positive Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Our Mobile Technologies Policy is an integral part of our Online Safety and AUP.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will consider the use of mobile technologies.

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	N/A	Yes	Yes
Internet only						
No network access						

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 cyber-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:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. 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/social media/local.
- 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 policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff may be used as permitted by the school principal, Ms Coyle.
- 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.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

Data Protection

Article 16: *You have the right to privacy.*

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.

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.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy 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:

	Staff & Other Adults			Pupils				
	Allowed.	Allowed at certain times.	Allowed for selected staff.	Not allowed.	Allowed	Allowed at certain times.	Allowed with staff permission.	Not allowed.
Communication Technologies								
Mobile phones may be brought to the school.	X							X ¹
Use of mobile phones in lessons.		X						X
Use of mobile phones in social time.	X							X
Taking photos on mobile phones/cameras.		X						X
Use of other mobile devices eg tablets, gaming devices.	X						X	
Use of personal email addresses in school, or on school network.	X							X
Use of school email for personal emails.				X				X
Use of messaging apps.		X						X
Use of social media.		X						X
Use of blogs.		X						X

^{X1} Pupils will keep mobiles in the school office.

^{X2} If photos are taken on a personal phone they must be transferred to a school device and deleted before the end of the day.

^{X4} For school use only. School Twitter or Facebook accounts.

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

- The official school email service 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 (e.g. by remote access).
- Users must immediately report to Mrs Kearney/Ms Coyle - 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, Teams, School Twitter, School Facebook, 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 Foundation Stage and Key Stage 1, while pupils at Key Stage 2 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will 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 - Protecting Professional Identity

Article 16: *You have the right to privacy.*

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.
- Private opinions should not be attributed to the school.
- 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 is:

- A process for approval by the Board of Governors.
- 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 a personal social media account. 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.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school Principal will 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 Mrs Kearney and Ms. Coyle 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 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:

		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 eg Youtube		X			

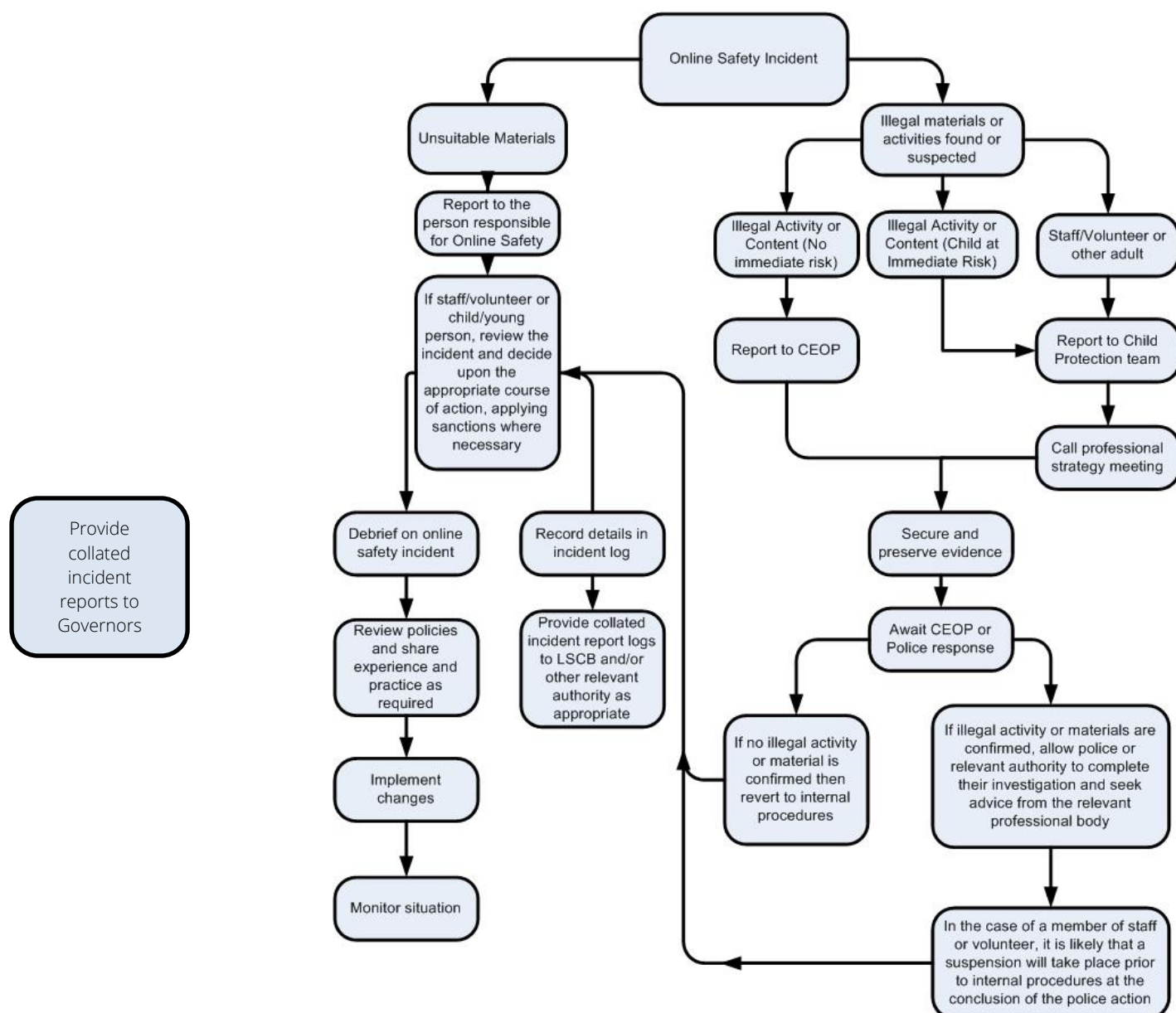
Responding to Incidents of Misuse

Article 19: *You have the right to be protected from being hurt and mistreated in body or mind.*

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").

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 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 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).
- 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 Education Authority /DENI;
 - 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 (Appendix 1) 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/tutor	Refer to ICT Curriculum Leader	Refer to Principal	Refer to Police	Refer to technical support staff for	Inform parents / carers	Removal of network/internet access rights (which may be for a temporary	Warning	Further sanction eg
Pupils Incidents									
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons.	X	X	X			X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device.	X	X	X			X		X	X
Unauthorised/inappropriate use of social media/messaging apps/ personal email.	X	X	X			X	X	X	X
Unauthorised downloading or uploading of files.	X	X	X			X	X	X	X
Allowing others to access school network by sharing username and passwords.	X	X	X				X	X	X
Attempting to access or accessing the school network, using another pupil's account.	X	X	X				X	X	X
Attempting to access or accessing the school network, using the account of a member of staff.	X	X	X			X	X	X	X
Corrupting or destroying the data of other users.	X	X	X			X	X	X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X	X			X	X	X	X

	Actions / Sanctions							
	Refer to Member of Safeguarding Team	Refer to Principal	Refer to Employing Authority (Governors)	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action which may include suspension or
Staff Incidents								
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X			X
Inappropriate personal use of the internet/social media /personal email e.g. during working hours.		X	X			X		
Unauthorised downloading or uploading of files.		X	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					X
Careless use of personal data e.g. holding or transferring data in an insecure manner.		X				X		
Deliberate actions to breach data protection or network security rules.		X	X	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.		X	X		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X	X				X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils.	X	X	X	X				X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.		X	X					X
Using proxy sites or other means to subvert the school's filtering system.		X	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
Breaching copyright or licensing regulations.		X	X			X		
Continued infringements of the above, following previous warnings or sanctions.		X	X				X	X

Acknowledgements

This policy was developed using the 360-degree Safe Online Safety Self-Review Tool and SWGFL (South West Grid for Learning Trust).