e-Safety Policy

Principal: Fionnguala Mc Cotter

Chairperson:

Date of Last Review: 2019

Date of Next Review:

Development/Monitoring/Review of this Policy

This e-safety policy has been developed by;

- Conchúr Keenan (ICT-Coordinator)
- Fionnguala Mc Cotter (Principal)

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

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Board of Governors Sub Committee on:	May 2019
The implementation of this e-safety policy will be monitored by the:	ICT Coordinator, Principal, SMT, teaching staff
Monitoring will take place at regular intervals:	May (annually)
The Board of Governors will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	June (annually)
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	May 2020
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Board of Governors Gateway PSNI

The school will monitor the impact of the policy using:

- Logs of reported incidents (recorded in principal's office diary)
- Surveys/questionnaires of pupils, parents/carers and staff.

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

The school will deal with such incidents within this policy and associated policies;

- *Positive Behaviour Policy*
- *Pastoral Care Policy*
- *Child Protection and Safeguarding Policy*
- *Special Educational Needs Policy*
- *Health and Safety Policy*
- *Relationships and Sexuality Education*
- *E-Safety Policy & Acceptable Use of Internet Policy*
- *Outings Policy*
- *Staff Code of Conduct*
- *Code of Conduct for Parents*
- *Complaints Procedures*
- *Transitions Policy*
- *Safe Handling*

and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities
The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Board of Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Child-Protection member of the Board of Governors has taken on the role of E-Safety Governor as part of their duties. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinator

- Regular monitoring of e-safety incident logs
- Reporting to the Board of Governors

Principal and Senior Leaders:

- The Principal a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Coordinator.
- The Principal and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Education Authority procedures).
- Principal and Senior Leaders are responsible for ensuring that the ICT Coordinator receives suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The ICT Coordinator and Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the ICT Coordinator

E-Safety Coordinator:

Conchúr Keenan is the named ICT/E-Safety Coordinator. The E-Safety Coordinator;

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the C2K, EA, Capitia, IMSGOL and other relevant bodies.
    - Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (ICT log in office)
    - Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
    - Attends relevant Governor meetings
    - Reports regularly to Senior Leadership Team
    - Reports all Child-Protection issues arising from the misuse of technology to the Child Protection officer (Fionnguala McCotter or Claire Donnelly/Conchúr Keenan)

Network Manager (C2K):

C2K are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the Virtual Learning Environment (My-School) and email is regularly monitored in order that any misuse/attempted misuse can be reported to the principal or E-Safety Coordinator for investigation.
- That monitoring systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and accepted the Staff Acceptable Use Policy (AUP). Competed on the first login each academic year to the C2K network.
- They report any suspected misuse or problem to the principal or E-Safety Coordinator for investigation.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems (My-school, SeeSaw, Google Classroom, Fronter or c2k e-mail).
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the e-safety and acceptable use policies.
- 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.
- They must ensure that Youtube videos or any other streamed media is appropriate.
- Children are not permitted to bring electronic devices into school. If a child must have a mobile phone it must be left with the school office until home time.
- Teaching Staff have been allocated a class iPad. This is to be used for school related tasks only. Staff are permitted to bring the devices home but must sign the device

out/in. Only educational apps may be installed on the iPads via the schools Apple Account, new/additional apps may be summited for installation via the Principal/ICT Coordinator.

- Teaching staff may need to use personal devices in the following circumstances;

❖ in areas of the school where there is no Wi-Fi,

❖ while on school trips, in the yard, PE lessons in Shaftsbury Community Centre

❖ To ring the office in the absence of a school phone system.

❖ Staff will not store school photos or videos on phones.

❖ Other exceptional circumstances based upon risk assessment/approval from principal. Recorded in the ICT log.

Child Protection Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to inappropriate materials.
- Inappropriate on-line contact with adults.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Pupils

- Are responsible for using the school's technology systems in accordance with the Pupil Acceptable Use Policy (Provided by C2K on initial login)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

- Should not bring personal devices to school unless necessary. They should give their device to the class teacher to be stored in the office until home time.

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' meetings, newsletters, letters, website and information about e-safety. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Interaction with staff through school social media, SeeSaw, Google Classroom etc.
- Their children's personal devices in the school.
- Parents are expected to communicate with staff in line with the Parent's Code of Conduct.
- Parents should not expect staff to reply to online communications (Seesaw etc.) Staff are available between the hours 8.30am to 4.30pm. Messages sent after 4.30pm will be answered at the teacher's earliest convenience.

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA (provided via C2K's temporary user profile) before being provided with access to school systems. External users will be permitted at the discretion of the principal.

Policy Statements

Education – 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of ICT and PDMU lessons.
- Key e-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 helped to understand the need for the student/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 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, 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 the ICT Coordinator or principal 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. This must be recorded with a clear start and end time in the ICT log.

Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and 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

- Letters, newsletters, web site, SeeSaw
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their e-safety provision (possibly

supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)

Education & Training – Staff/Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly (May each year or as needed) It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The ICT Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings or training days.
- The ICT Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Department of Education, EA or other relevant organisation.
- Participation in school training/information sessions for staff or parents.

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 e-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 (P3-7) will be provided with a username and secure password by the ICT Coordinator who will keep an up to date record of users and their usernames. Foundation stage pupils may use a group login to be managed by class teacher Users are responsible for the security of their username and password and will be required to change their password every (90 days).
- The ICT Coordinator 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. Subject specific licences are the responsibility of the subject Coordinator (e.g. Lexia), the ICT coordinator will assist the installation if required.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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 (see appendix for more details)
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for staff and pupils)
- Users must report any actual/potential technical incident/security breach to the ICT Coordinator and record the incident in the ICT log (stored in the office).
- 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.
- The provision of temporary access of “guests” (external support, trainee teachers, substitute teachers, visitors) onto the school systems can only be given by the principal, ICT coordinator or SMT. All guests must be recorded in the visitors log with; name, purpose of visit, start date and end date.
- Personal use of school systems by users (staff, pupils, community users) is prohibited. Staff may bring a laptop/iPad or tablet home for work proposes only.
- Downloading executable files and installing programmes on school devices must be approved by The ICT Coordinator, subject coordinator and principal and meet C2k requirements. Staff must record in the ICT log the proposed use of new software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Staff are responsible for the appropriate use of CDs, DVDs and portable memory devices, advice should be sought on the use of such materials from the ICT coordinator.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies. Pupils are not permitted to BYOD but may be required to use a personal device for homework etc.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

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.

- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in 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 permitted 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 non-teaching staff should not be used for such purposes. Teaching staff may use mobile phones in certain circumstances as outlined n page 5
- 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, permission will be sought from parents/carers.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

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 (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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 is a policy for reporting, logging, managing and recovering from information risk incidents
- 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 (G Suite)
-

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 where possible.
- Sensitive data (SIMS data, child protection issues etc.) is not permitted to be copied to portable devices that cannot be password protected. Staff must seek permission from the principal before any sensitive data is copied.
- 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				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons		✓		✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/cameras		✓		✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
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 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/SeeSaw to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content**.** These communications may only take place on official (monitored) school systems i.e. SeeSaw, Google Classroom and website. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while/pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-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 - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in Code of Values and Professional Practice (GTCNI, 2018). While, DE Circular 2016/27 Internet Safety, provides a set of guiding principles for keeping pupils and the wider school community safe online and for prioritising online safety within the school's preventative education curriculum and overall Safeguarding Policy.

All schools 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 minimize risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: 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.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

Unsuitable/inappropriate 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 school or outside 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	
	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)		✓				
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping/commerce			✓			
File sharing			✓			

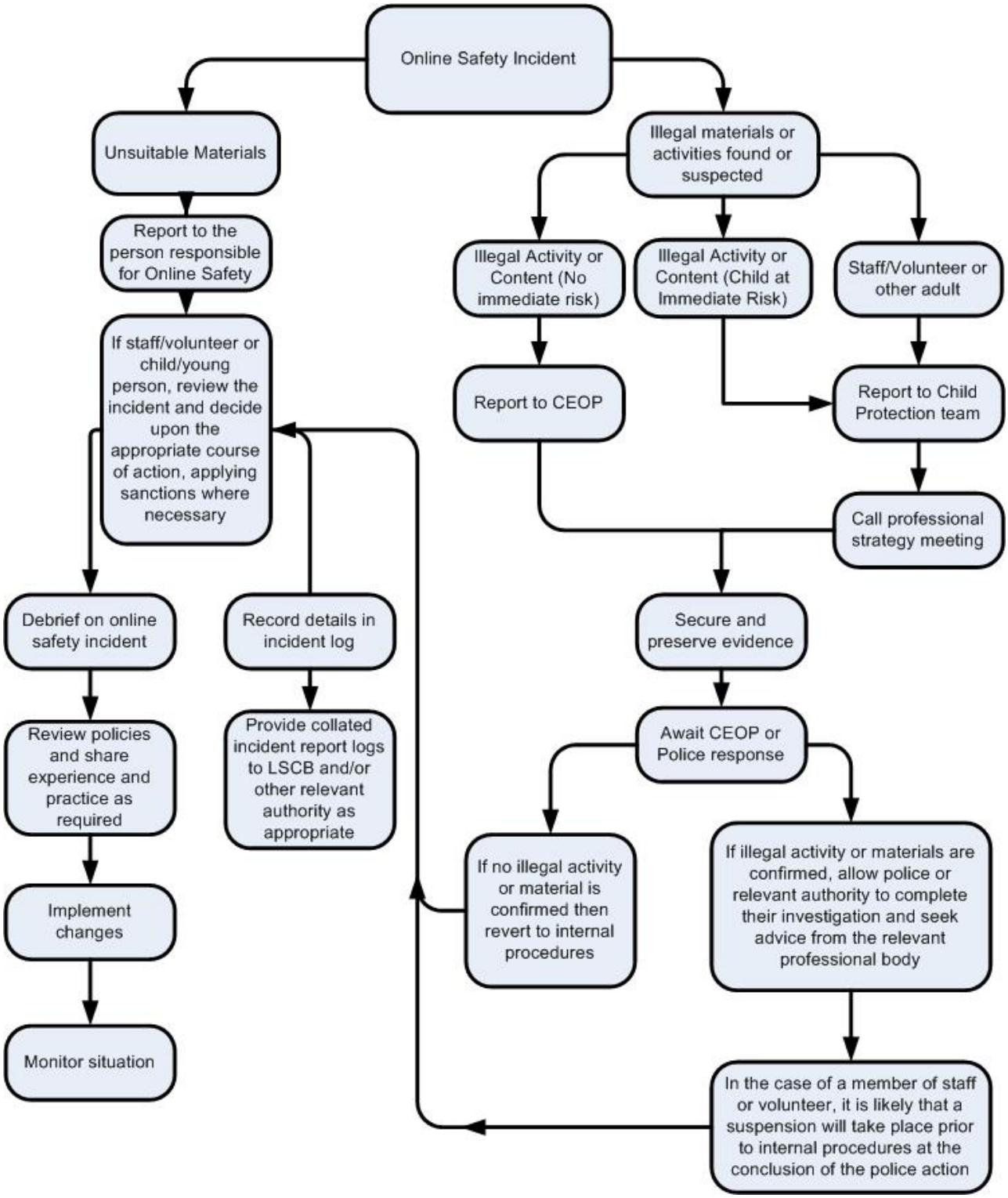
Use of social media				X	
Use of messaging apps (Skype for Business)		✓			
Use of video broadcasting e.g. Youtube, streaming		✓			

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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 Education Authority
    - Police involvement and/or Gateway referral
- 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
    - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & 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:

Pupils	**Actions**								
Incidents:	Refer to class teacher	Refer to ICT Coordinator	Refer to Principal	Refer to Police	Refer to technical support (C2K)	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
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 use of mobile phone/digital camera/other mobile device	✓								
Unauthorised 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 pupil's 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			✓						
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 **Actions/Sanctions**

Incidents:	Refer to ICT Coordinator	Refer to principal	Refer to EA	Refer to Police	Refer to ICT Coordinator for action re filtering etc	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	✓							
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 warnings or sanctions	✓	✓					✓	✓

Appendix