eSafety/Online Safety Policy (draft)

Introduction

What is eSafety?

- eSafety is short for electronic safety.
- It highlights the responsibility of the school, staff, governors and parents/carers to mitigate risk through reasonable planning and actions. eSafety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

eSafety in the school context

- Is concerned with safeguarding children and young people in the digital world
- Emphasises learning to understand and use new technologies in a positive way
- Is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online
- Is concerned with supporting pupils to develop safer online behaviours both in and out of the school
- Is concerned about helping pupils recognise unsafe situations and how to respond to risks appropriately

(Guidance taken from DE Circular 2013/25)

Rationale

We in Lismore recognise there is a duty of care for any persons working with children and educating all members of the school community on the risks and responsibilities of eSafety falls under this duty.

This eSafety policy has been developed by an eSafety working group made up of:

- ICT Manager
- Data Manager
- ICT Coordinator
- Member of Safeguarding Team

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

Communicating this policy:

This policy is available on the school website for parents, staff and pupils to access when and as they wish. Hard copies are available on request. eSafety posters are displayed throughout the school and eSafety is integrated into the curriculum.

This eSafety policy was approved by the *Board of Governors* on:	*Insert date*
The implementation of this eSafety policy will be monitored by the:	eSafety Working Party
Monitoring will take place at regular intervals:	*at least once a year*
The Board of Governors will receive a report on the implementation of the eSafety policy generated by the monitoring group.	*at least once a year*
The eSafety 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 eSafety or incidents that have taken place. The next anticipated review date will be:	*Insert date*
Should serious eSafety incidents take place, the following external persons / agencies should be informed:	*C2K,Child Protection Support Service for Schools, Gateway Service for Children's Social Work Team, PSNI*

The school will monitor the impact of the policy using:

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

Scope of the Policy
This policy applies to all members of the Lismore Community (including staff, pupils, volunteers, parents/carers, visitors, community users)

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about eSafety incidents and monitoring reports. The Designated Governor for Child Protection will provide the lead on eSafety.

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Team.

- The Principal and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see appendix 1- flow chart on dealing with eSafety/Online Safety incidents.)

- The Principal and Senior Leaders are responsible for ensuring that the eSafety Team and other relevant staff receive suitable training to enable them to carry out their eSafety roles and to train other colleagues, as relevant.

- The 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 eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Appropriate external agencies will be consulted in this process.

eSafety Team:

- Takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- provides training and advice for staff
- liaises with external agencies as appropriate
- liaises with school technical staff
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments (see appendix 2, log)
- reports to Senior Leadership Team and Governors

ICT Manager:
The ICT Manager is 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 eSafety technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as appropriate
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation / action / sanction
- that monitoring software / 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 eSafety matters and of the current school's eSafety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)(see appendix 3, Staff AUP)
- they report any suspected misuse or problem to the Principal, eSafety Team, Safeguarding Team for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the eSafety 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

Safeguarding Team

should be trained in eSafety 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy(see appendix 3,Pupil AUP)
- 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 eSafety practice when using digital technologies out of school and realise that the school's eSafety 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 newsletters, letters, website / VLE and information about eSafety campaigns. Parents and carers will be encouraged to support the school in promoting good eSafety practice.

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (See appendix 4 community user AUP)

Cyber Bullying

Developments in Information and Communication Technology (ICT) have made incidents of cyber bullying more widespread. This form of bullying is considered within Lismore's anti-bullying policy and pastoral services as well as this policy. Cyber Bullying can take many forms including
Email-nasty or abusive emails which may include viruses or inappropriate content
Instant Messaging (IM) and Chat Rooms-potential to transmit threatening or abusive messages
Social Networking Sites-typically includes the posting and publication of nasty or upsetting comments on another user's profile
Online Gaming-abuse or harassment of someone using online multi player game sites
Mobile phones-examples can include abusive texts, video or photo messages. Sexting can also occur, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people
Abusing Personal Information-may involve posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber bullying may appear to provide anonymity for the bully, most messages can be tracked back to the creator and pupils are reminded that cyber bullying can constitute a criminal offence. It is the policy in Lismore for staff **not to look through a pupil's mobile phone or read information or look at photographs on a pupil's social networking site.** If a parent/guardian discovers that their child is being bullied via the internet or mobile phone, the school advises that they should seek advice from the PSNI. If the bullying has an impact on the behaviours or relationships between pupils in school, staff will investigate the incident in line with the Behaviour for Learning Policy and Anti bullying Policy and procedures. Pupils will be encouraged to report incidents of cyber bullying to both the school and, if appropriate the PSNI to ensure the matter is properly addressed and the behaviour ceases.
Logs of cyber bullying incidents will be kept to monitor the effectiveness of preventative activities, to review and ensure consistency in investigations, support and sanctions.

Management of Risk Assessment

Lismore will perform risk assessments on the technologies within the school to ensure that we are fully aware of and can mitigate against the potential risks involved with their use. The school will take all reasonable precautions to ensure that users access only appropriate material. Pupils need to become 'Internet Wise' and ultimately good 'digital citizens'. Pupils need to know how to cope if they come across inappropriate material or situations online. These risks have been defined and categorised by the National Children's Bureau NI as follows:

Content risks - the young person is exposed to harmful material
Contact risks - the young person participates in adult initiated online activity
Conduct risks - the young person is a perpetrator or victim in peer to peer exchange
Commercial risks - the young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

However due to the international scale and linked nature of internet content and while all necessary safeguarding procedures and policies are in place, it is not possible to guarantee that unsuitable material will never appear on a school computer. **The school cannot accept liability for the material accessed, or any consequences of Internet access.**

Education – pupils

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

- A planned eSafety curriculum should be provided as part of Computing / PD / other lessons and should be regularly revisited.
- Key eSafety messages should be reinforced as part of a planned programme of assemblies.
- 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 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, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Manager 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 eSafety 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:

- Letters, Newsletters, School website, VLE
- High profile campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk / www.childnet.com/parents-and-carers (see appendix 5 for links)

Education – The Wider Community

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

- The school website will provide eSafety information for the wider community

Education & Training – Staff / Volunteers

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

eSafety training will be included as part of our Safeguarding training programme

All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Agreements.

This eSafety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

Training – Governors

Governors should take part in eSafety awareness sessions, with particular importance for those who are members of sub committee for child protection. This may be offered in a number of ways:

- Attendance at training provided by the EA or other relevant organisation.
- Participation in school information sessions for staff or parents. This may include attendance at assemblies.

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 eSafety 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 will be provided with a username and secure password by (J Furphy) 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 (three months).

- (J Furphy) 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.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. (see appendix 2)
- 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 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. (see appendix 6, personal use of school devices e.g. ipads)
- An agreed policy with C2K is in place 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 (e.g. 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.

Bring Your Own Device (BYOD)
(see appendix 7 for BYOD Policy)

- 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.
- Any device loss, theft 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 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. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their

own personal use .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 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix 4)
- Pupil's work can only be published with the permission of the 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 9, 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 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 which ensure that such data 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.

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	Not advised	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/devises as a resource in lessons	✓						✓	
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones / cameras / other devices e.g. tablets				✓				✓
Use of personal email addresses in school, or on school network	✓						✓	
Use of school email for personal emails	✓	✓						✓
Use of messaging apps				✓				✓
Posting on school approved social media	✓							✓

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.
- Users must immediately report 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.

Social Media - Protecting Professional Identity

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
- 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 eSafety Team to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

Unsuitable / inappropriate activities

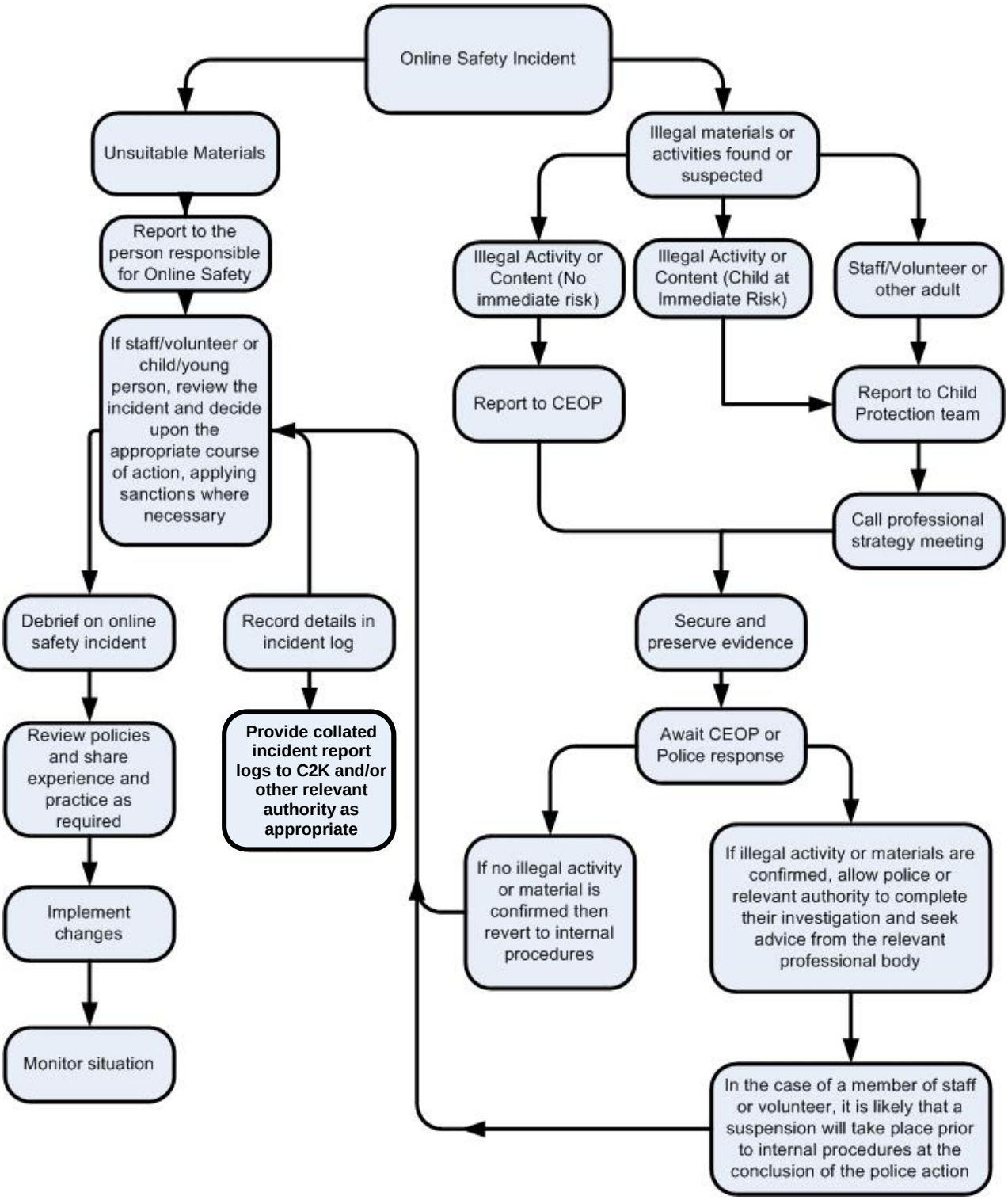
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

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 (e.g. 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	
Posting on school approved social media				X		
Use of messaging apps					X	
Use of video broadcasting e.g. YouTube		X				

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix 1) for responding to online safety incidents and report immediately to the PSNI.



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 – 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
    - 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 intended that incidents of inappropriate misuse will be dealt with through the Behaviour for Learning Policy.

Deliberately accessing or trying to access material that could be considered illegal will result in a referral to the Principal and PSNI.

The following are deemed as incidents of inappropriate misuse:

- 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 student's / 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 '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.

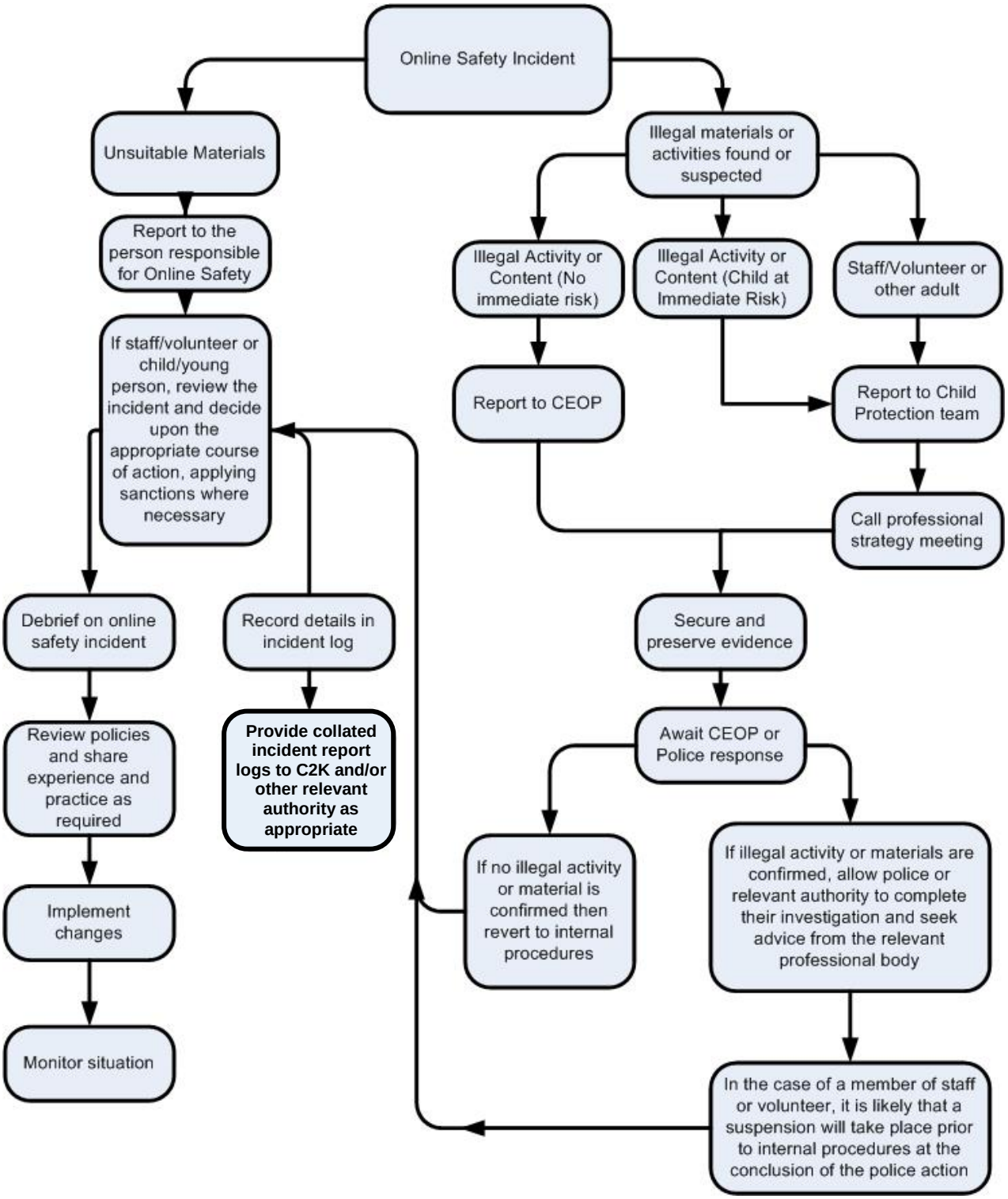
School Actions & Sanctions for Staff

The following actions are considered unacceptable.

Any breaches will result in a referral to the Principal and other relevant authorities as appropriate.

- 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 students / 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.

Flow Chart for Responding to eSafety/Online Safety Incident.



Links for Parents

www.swgfl.org.uk

www.saferinternet.org.uk

www.childnet.com/parents-and-carers