St Louis Grammar School Kilkeel

E-Safety Policy

2026-2027

Last Reviewed: September 2025

Reviewed by: Mr T. Brown

Date of Review: September 2027

Introduction

This E-Safety and Bring Your Own Device Policy outlines the governance structure and specific regulations necessary to support the operation of the school's online environment. This document should be read in conjunction with the school’s overarching **School Online Safety and Acceptable Use Policy**.

Scope of the Policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents, carers, visitors, and community users, who access or use school Information and Communication Technology (ICT) systems, both within and outside the school premises.

The school reserves the authority to regulate the behaviour of pupils off the school site where inappropriate conduct, including cyber-bullying or other online safety incidents, is linked to their membership of the school. Such incidents will be addressed under this policy and the associated positive behaviour and anti-bullying protocols.

Roles and Responsibilities (Governance and Oversight)

The governance of e-Safety and the school’s digital infrastructure is managed by designated staff roles:

Governors: The Board of Governors are responsible for the formal approval of the E-Safety Policy framework and regularly reviewing its effectiveness through monitoring reports and e-safety incident statistics received by the Governors Sub-Committee.

Principal and Senior Leadership Team (SLT): The Principal holds the ultimate duty of care for ensuring the safety of the school community. This responsibility is delegated to the E-Safety Co-ordinator. The Principal and SLMT ensure that all staff receive necessary training and oversee the support system for colleagues involved in network monitoring. They receive regular reports from the E-Safety Co-ordinator.

E-Safety Coordinator: The E-Safety Coordinator leads the E-Safety Committee and manages day-to-day e-safety issues, including establishing and reviewing e-safety documents in coordination with technical and pastoral staff. This role ensures staff awareness of incident procedures, provides training, liaises with external bodies, and maintains a log of all reported incidents to inform future policy development.

C2K Manager/Technical Staff: The C2K Manager (or equivalent technical staff) ensures the school's technical infrastructure is secure against misuse or malicious attacks, complies with necessary technical requirements (including those set by ENNI), and implements enforced password policies. They oversee the implementation of the ENNI filtering policy and monitor network usage, reporting misuse to the SLT and E-Safety Coordinator for action.

Teaching and Support Staff: All staff must maintain up-to-date awareness of digital safety and adhere to the Online Safety and Acceptable Use Policy. They are responsible for embedding online safety principles across the curriculum, monitoring digital device use in lessons, and immediately reporting any suspected misuse or problems to senior staff for investigation.

Child Protection / Safeguarding Officer: The Safeguarding Team receives training in online safety issues and is aware of the serious potential for child protection issues arising from activities such as sharing personal data, accessing illegal materials, inappropriate contact, grooming, and cyber-bullying.

E-Safety Committee: The E-Safety Committee is a consultative group with school community representation. Its functions include monitoring the e-safety policy's impact, reviewing filtering changes, consulting stakeholders (including parents and pupils), and monitoring incident logs, cyber-bullying (in conjunction with the Designated and Deputy Designated Child Protection Officers), and the safe use of data across the school.

Technical Management and System Security

The effective functioning and security of the school's digital network are maintained through the following procedures:

- **Infrastructure Management:** Technical systems undergo regular reviews and audits to ensure security. Servers, wireless systems, and cabling are securely located with restricted physical access.
- **User Access:** All users are provided with a unique username and secure password and are required to change their passwords regularly.
- **Filtering and Monitoring:** Internet access is filtered for all users through the C2K network, including the enforcement of the Internet Watch Foundation's list for illegal content. Internet use is consistently logged and monitored. Technical staff regularly monitors user activity and records it, and users are made aware of this in the Acceptable Use Agreement.
- **Security Breaches:** An agreed system is in place for users to report any actual or potential technical incidents or security breaches immediately to the relevant designated person.
- **Data Security:** Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured, in adherence to the school's Data Protection Policy.

Bring Your Own Device (BYOD) Conditions

The use of personal mobile devices (BYOD) within the school environment is governed by clear expectations to ensure compatibility and safeguard the school network and this section must be read in conjunction with schools' Online Safety and Acceptable Use Policy.

Device Requirements and Management

1. **Approval and Policy Adherence:** Pupils must obtain written permission from parents or carers to use their own devices for accessing the filtered wireless network or the school network. Devices must be used solely for **educational purposes**.
2. **Compatibility and Inspection:** Devices must be compatible (e.g., Windows-based laptops, Apple Macintoshes, iPads, or tablets). They may be checked by ICT staff prior to use for compatibility and to ensure there is **no existing unsuitable material** stored on the device.
3. **Network Access:** Only filtered Internet connections provided by the school (C2K network or school non-C2K wireless network) may be used on the school premises. The use of mobile broadband, personal hotspots, or Bluetooth connections for network access is **prohibited**.
4. **Security Software:** If connecting to the network, the device must have an **up-to-date anti-virus/internet security product installed** to comply with the acceptable use terms.
5. **Monitoring and Inspection Consent:** All users who sign the BYOD agreement agree to the **monitoring** of their internet, cloud, and email usage to prevent misuse and protect school data. The school retains the right to **check devices at any time** for inappropriate use and, in extreme cases, the Principal may authorise the copying, erasing, or remotely wiping of the entire device (including personal data).
6. **Liability:** The user is **solely responsible** for the correct care, safety, and security of the device while in transit or at school. The school **accepts no liability** for any loss or damage to personal devices used on school premises or during school activities. Users are recommended to ensure they have appropriate private insurance cover.
7. **Data Storage (Staff):** Staff **must not** store electronic copies of sensitive personal information on any personally owned portable or non-portable device, or on portable storage devices.
8. **Electrical Safety:** Portable mains powered electrical items owned by staff or pupils must not be brought into school unless they have a current electrical safety test certificate (within the last 12 months).

Use of Digital and Video Images

To mitigate risks associated with sharing digital images (which remain available indefinitely and may lead to cyber-bullying or reputational damage):

1. **Consent:** Written permission from parents or carers must be obtained before publishing photographs of pupils on the school website or public channels.
2. **General Image Use:** Photographs published that include pupils will be carefully selected and comply with good practice guidance. Full names of pupils will not be used in association with photographs or videos.
3. **Staff Use of Devices:** Staff must take digital or video images to support educational aims **only on school equipment**. Personal devices must not be used for recording pupils.
4. **Pupil Conduct:** Pupils **must not** take, use, share, publish, or distribute images or videos of others without their explicit permission.
5. **Compromising Images:** If a member of staff inadvertently captures a compromising picture that could be misused, they must **delete it immediately** and inform the Designated Safeguarding Lead.

Social Media and Professional Identity (Staff)

Staff are advised on acceptable conduct related to social media to protect professional identity and school reputation:

1. **Pupil Contact:** Staff **must not** add current or past students to their online personal social networks, as this may inadvertently provide indirect links to current students.
2. **Privacy and Content:** Staff must regularly check their security settings on personal profiles. They must ensure that publicly available information about them is **accurate and professional**. Inappropriate content, unprofessional material, or anything defamatory towards the school or its stakeholders is considered a disciplinary matter.
3. **Confidentiality:** Staff must not engage in online discussions on personal matters relating to members of the school community. They must ensure that confidentiality and data protection regulations are maintained at all times.
4. **Reporting Abuse:** If staff become aware of unpleasant comments posted on public websites about themselves or colleagues, they must **immediately report such abuse to the Principal** for guidance on handling the incident and reporting to the platform/authorities.

Incident Management

In the event of misuse or a policy breach:

1. **Reporting:** Any suspected misuse, problem, or inappropriate content must be reported immediately to the E-Safety Coordinator or Principal/SLMT.
2. **Illegal Activity:** If illegal activity or illegal content (such as child abuse images) is suspected, all monitoring or investigation must halt, and the incident must be **reported immediately to the Police (PSNI) and Social Services**.
3. **Sanctions:** Breaches of policy will be dealt with severely, in line with the procedures outlined in the overarching School Online Safety and Acceptable Use Policy and the Positive Behaviour Policy. Sanctions may include immediate withdrawal of network access, disciplinary action (including suspension or expulsion in cases of serious misconduct), and involvement of external agencies.

Principal and SLMT

The Principal and SLMT:

- The Principal has 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 E-Safety Co-ordinator.
- The Principal 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 the Appendix 2– "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal 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 and Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator

The e-Safety Coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- 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 Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

C2K Manager

The C2K Manager / Technical Staff / Co-ordinator for ICT / Computing 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 e-safety technical requirements and those of the ENNI / other relevant body E-Safety Policy / Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the ENNI 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; E-Safety Coordinator investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

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 signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to Principal / Senior Leader / E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / 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 students / 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

Child Protection / Safeguarding Officer

The safeguarding team should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Principal and Governing Body. The terms of reference for the committee can be found in Appendix 4 of this document.

E-Safety Committee Members:

Members of the E-safety Committee will assist the E-Safety Coordinator (or other relevant person, as above) with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Online Safety and Acceptable Use Policy
- 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 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

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' evenings, newsletters, letters, website / GOOGLE CLASSROOM and information about national / local e-safety campaigns / literature. 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
- access to parents' sections of the website / GOOGLE CLASSROOM and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / GOOGLE CLASSROOM as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / 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 Computing / PD / Assemblies and other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, GOOGLE CLASSROOM
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day

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 eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision

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. 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 E-Safety Coordinator / Officer (or other nominated person) 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 / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) 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 sub committee / 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 Local Authority / National Governors Association / 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 will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg school safe)
- Internet access is filtered for all users. Illegal content is filtered by ENNI 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
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitors and records 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, 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.
- An agreed policy is in place for the provision of temporary access of “guests” (eg 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.
- An agreed policy 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 (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.

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.

- 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
- Students / 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 students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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 students / 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 eg on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 students / 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / 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 students / pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

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:

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 students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg 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 students / pupils or parents / carers (email, chat, GOOGLE CLASSROOM 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.
- Students / 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

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				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

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 (in Appendix 2) 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 / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - 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 / academy 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.

Appendix 1 – Reporting templates

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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

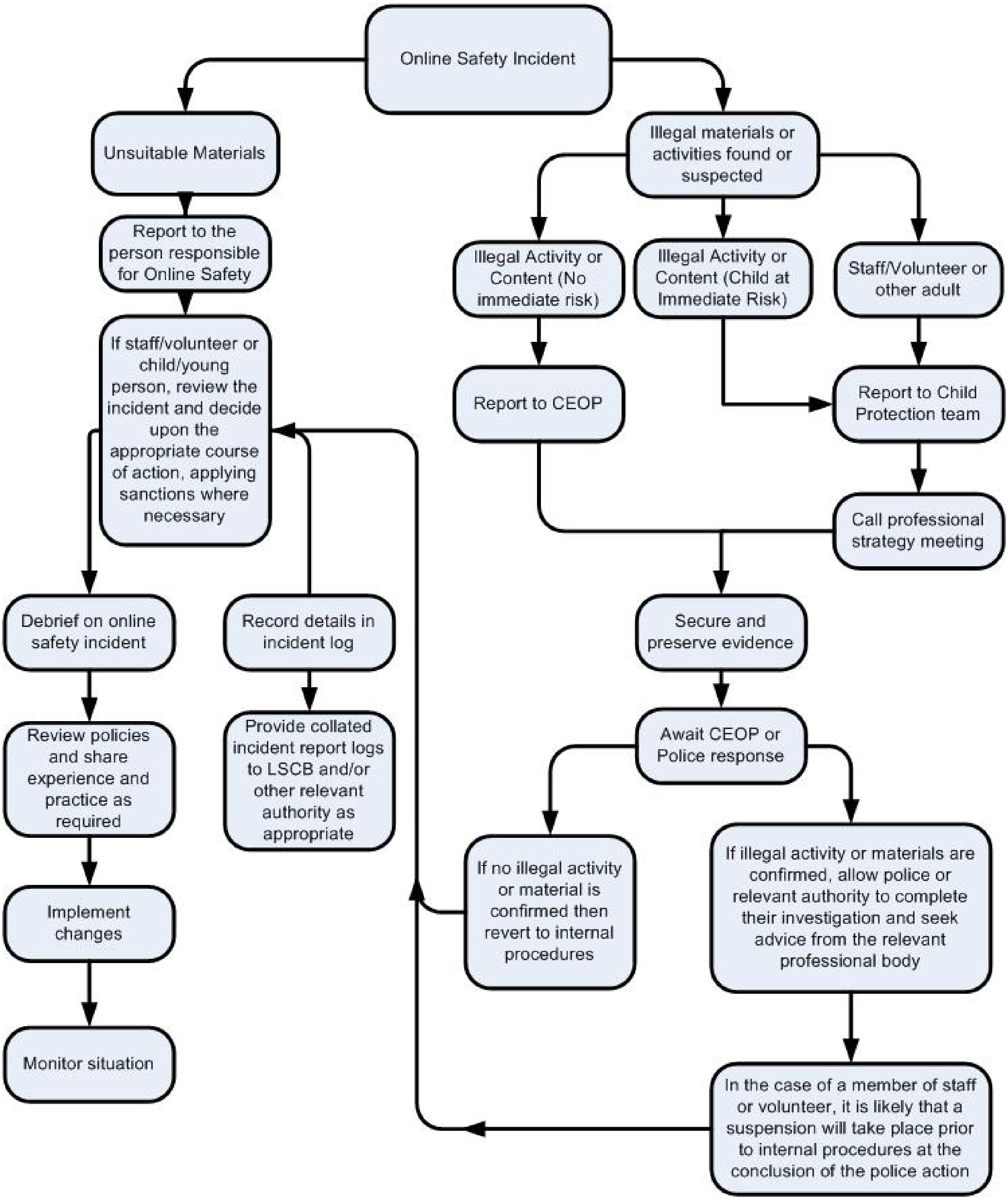
Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Template Reporting Log

Signature	
Incident Reported by	
Action taken and by whom?	
Incident	
Time	
Date	

Appendix 2 - Responding to incidents of misuse


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

Appendix 3 - Relevant Laws pertaining to Acceptable use and e-safety

Schools should be aware of the legislative framework under which this Online safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

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".
- It has a Data Protection 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 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.

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 (below) once it has been transferred or its use is complete

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Principals, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance -

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Appendix 4 - Online e-Safety Committee Structure and Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the [school] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The online safety committee will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member- Mr T Brown
- Child Protection/Safeguarding officer- Miss Caroline King
- Teaching staff member- Mr A O'Brien (ICT HOD)
- Support staff member- Mr Sean Haughian
- Online safety coordinator- MrT Brown
- Governor- TBC
- ICT Technical Support staff- Mr Sean Haughian

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON- Mr T Brown

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. DURATION OF MEETINGS

Meetings shall be held once per term for a single teaching period. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

The functions of the Online Safety Committee are to assist the Online safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:

  - Staff meetings
  - Student / pupil forums (for advice and feedback)
  - Governors meetings
  - Surveys/questionnaires for students / pupils, parents / carers and staff
  - Parents evenings
  - Website/GOOGLE CLASSROOM/Newsletters
  - Online safety events
  - Internet Safety Day (annually held on the second Tuesday in February)
  - Other methods
  - To ensure that monitoring is carried out of Internet sites used across the school
  - To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
  - To monitor the safe use of data across the school
  - To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for St. Louise Grammar School have been agreed

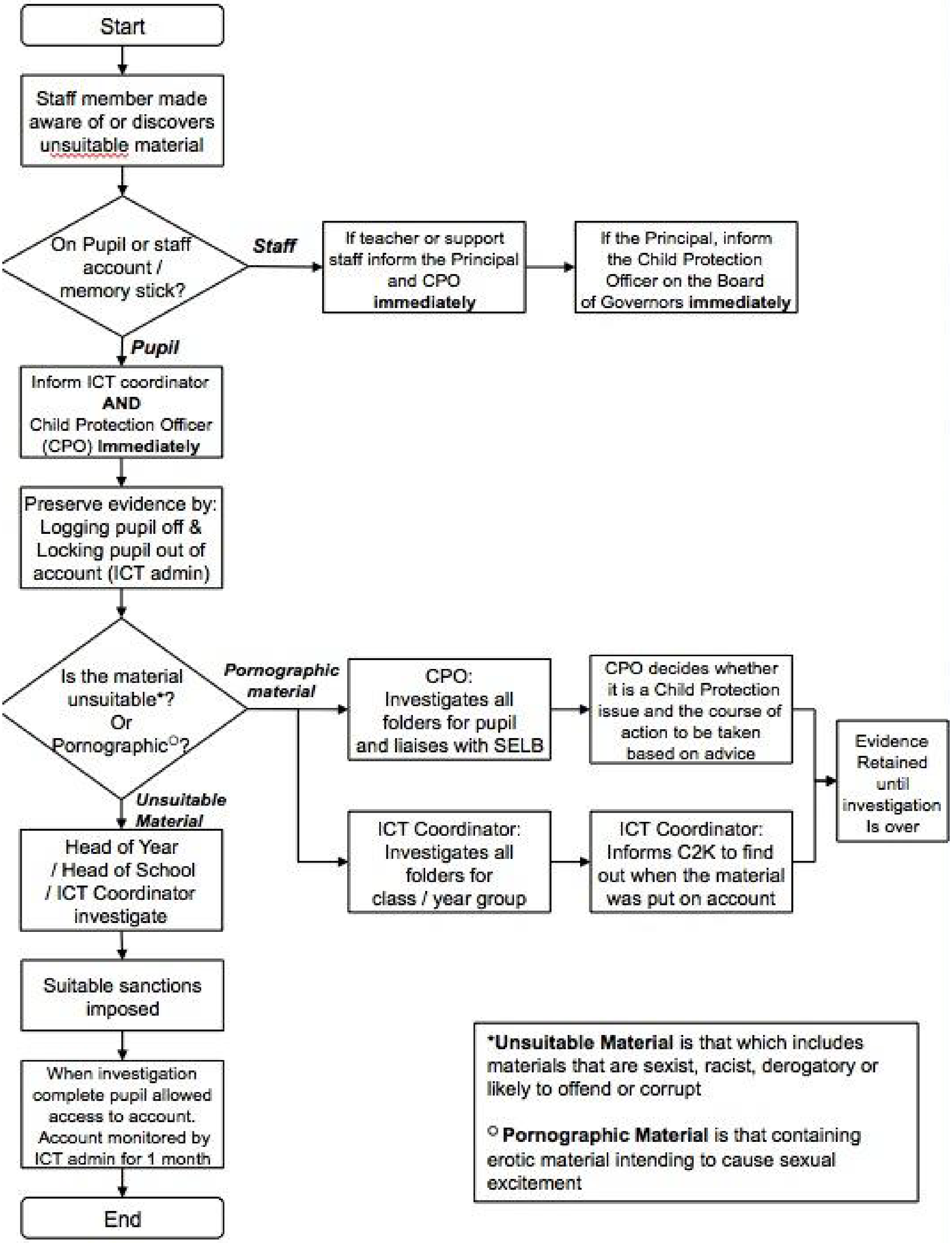
Signed by (SLT):

Date:

Date for review:

Appendix 5 – Flow chart for responding to e-safety Incidents / e-Safety Protocol for IT staff

Protocol for the discovery of unsuitable* material found in pupil storage area


Start
Staff member made aware of or discovers unsuitable material
On Pupil or staff account / memory stick?
Staff
If teacher or support staff inform the Principal and CPO immediately
If the Principal, inform the Child Protection Officer on the Board of Governors immediately
Pupil
Inform ICT coordinator AND Child Protection Officer (CPO) Immediately
Preserve evidence by: Logging pupil off & Locking pupil out of account (ICT admin)
Is the material unsuitable*? Or Pornographic○?
Pornographic material
CPO: Investigates all folders for pupil and liaises with SELB
CPO decides whether it is a Child Protection issue and the course of action to be taken based on advice
ICT Coordinator: Investigates all folders for class / year group
ICT Coordinator: Informs C2K to find out when the material was put on account
Evidence Retained until investigation Is over
Unsuitable Material
Head of Year / Head of School / ICT Coordinator investigate
Suitable sanctions imposed
When investigation complete pupil allowed access to account. Account monitored by ICT admin for 1 month
End

***Unsuitable Material** is that which includes materials that are sexist, racist, derogatory or likely to offend or corrupt

○ **Pornographic Material** is that containing erotic material intending to cause sexual excitement

Appendix 6 - E-Safety protocol for staff

This protocol should be read in conjunction with the ‘E-safety and acceptable use policy’ as well as the ‘Flow Chart for responding to e-safety incidents’.

Periodically the Director of ICT or ICT technician will search through pupils’ storage areas for unsuitable material and will deal initially with the Child Protection Officer and, depending on the advice given, with the pupil and their tutor / head of year / head of school as regards a suitable sanction. If however a member of staff becomes aware that a pupil is storing unsuitable material in their work area they must follow the protocol below.

Procedures for discovery of inappropriate images found on a pupil’s storage area or a memory pen

All Staff

Follow procedures in the schools Acceptable use policy e.g.

1. Inform ICT coordinator **and** a member of the Safeguarding Team **immediately**. Members of the team will decide, in conjunction with SELB board personnel, who needs to be informed and who is to be involved.
2. Preserve evidence (Pupil to be logged off immediately)
3. If a pupil, review incident and decide on course of action and impose sanctions as necessary
4. If material is found on a member of staff’s area, inform the Principal **immediately**
5. Debrief the ICT coordinator if dealt with by the Child Protection Officer
6. Review polices and technical tools and share experience and practice as required
7. Monitor the situation

Lost memory pens

- If a memory pen is found it must be taken by a teacher to Room 33 and given to a member of the ICT staff
- **Under no circumstances are teachers to lend a memory pen to a pupil including the teachers own memory pens.**
- All lost memory pens to be kept in a central location: Room 33
- The date that the memory pen is found should be recorded by a member of the ICT staff
- The ICT coordinator will inspect the contents of the memory pen
- If inappropriate material is found, follow points 1-7 above
- The owner of the memory pen must be identified where possible
- The owner of the memory pen must be informed
- If no owner is found, after 1 month, the memory pen is wiped (full format) and destroyed

ICT department procedures

- **If material is on pupil’s area:**
  - Investigate all folders belonging to the pupils
  - Investigate all folders in the class / year group
  - Investigate all pupils’ work on servers
  - Inform C2K – try to find out when the material was put on the account

    - Record the location of the files, what date they were created, what date they were modified and if possible who the author of the files is
    - Preserve evidence in original location until the investigation is completed.
    - Once the investigation is complete, delete materials – If necessary in the presence of parents
    - Preserve any emails regarding the issue and forward to the ICT Coordinator

- **If material is on memory pen:**

    - Remove memory pen from pupil or if found by a pupil, record the name of the pupil and date
    - Remove images and record the location of the files, what date they were created, what date they were modified and if possible who is the author of the files
    - Delete materials
    - Preserve any emails regarding the issue

Unsuitable Internet use during lessons protocol

If a member of staff becomes aware that a pupil is either accessing unsuitable websites during a lesson or is undertaking non-permissible activities on the Internet during a lesson then they follow the protocol below. Unsuitable activity includes sites that allow pupils to play games.

- Warn the pupil that unless they close down their browser they will have their Internet access removed.
- If the pupil ignores this warning and continues to use the Internet for activities that have not been permitted during the lesson then the member of staff must ask the pupil to log off immediately.
- The member of staff must inform the Director of ICT immediately by telephone of the incident. If the Director of ICT is not available they must inform the ICT technician or alternatively a teacher from the ICT department.

The Director of ICT will:

- Disable the pupil's account until evidence can be secured if necessary (see above).
- Disable the pupil's access to the Internet for a minimum of one month or until the matter has been discussed with the pupils tutor / year head / head of school and a suitable sanction has been imposed.
- If the site that has been accessed appears to contain unsuitable material the Director of ICT will contact and request a record of the pupil's internet use from ENNI and inform the Child Protection Officer.
- If the site has bypassed the Internet filter then ENNI will be informed of the web address and the site will be banned within school.
- Inform other members of the ICT staff who are able to enable / disable accounts by email of the pupil's username to ensure that the account or Internet access is not activated in error until the incident is resolved.
- The Director of ICT will also investigate the pupil's storage area in case any unsuitable materials have been downloaded.

[1] Unsuitbale material includes materials of a Pornographic, racist, sexist or material likely to offend or corrupt; non-educational 'Games' and "Exe" files including screen savers; Any material not associated with school work / coursework.

Illegal material or activity protocol

If a member of staff becomes aware that a pupil has performed: illegal activity on the Internet; has downloaded illegal material from the Internet; or if a pupil is at risk from such materials or has put another pupil at risk from such materials then they must follow the protocol below:

- Ask the pupil quietly to move away from the computer, if possible ensuring they do not touch the computer or delete the evidence.
- Inform the Director of ICT immediately by telephone. If the Director of ICT is not available inform the ICT technician or alternatively a teacher from the ICT department.

The Director of ICT will:

- Take steps to preserve the evidence by printing out the unsuitable material or copying the material to a portable storage device.
- Ensure that the pupils account is disabled until an interview with the pupil is conducted by the Director of ICT and / or the head of year or head of school.
- Inform other members of the ICT staff who are able to enable / disable accounts by email of the pupils username to ensure that the account is not activated in error until the incident is resolved.
- If the material appears to have been obtained from the Internet from within school, the Director of ICT will contact and request a record of the pupils internet use from ENNI.
- If the material has been obtained from an unsuitable site that has bypassed the Internet filter then ENNI will be informed of the web address and the site will be banned within school
- Inform the principal or child protection office immediately who will in turn inform the relevant authorities as detailed in the ‘Flow Chart for responding to e-safety incidents’.

Whilst the incident is being investigated the pupil will no longer have access to the school network.