St Mary's E-Safety Policy

September 2023

To be reviewed: September 2024

E Safety Policy

Schedule for Development/Monitoring/Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or online incidents that take place.

The Local Governing Body will receive an update on the implementation of the E-Safety Policy annually and this will be discussed at Local Committee Meetings.
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 students, parents/carers and staff.

Scope of the Policy
This policy applies to all members of St Mary's Primary (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of St Mary's Primary ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and consequently the searching of electronic devices and the deletion of data (under section 85AC(6D)).

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

Roles and Responsibilities
The following section outlines the E-Safety roles and responsibilities of individuals and groups within St Mary's Policy

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

- Regular updates from the Digital Media Team
- Regular monitoring of E-Safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to relevant Governors on appropriate matters.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, although the day-to-day responsibility for E-Safety will be delegated to the Digital Media Team.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (see Appendix A for dealing with E-Safety incidents).
- The Headteacher/Senior Leadership Team are responsible for ensuring that the Digital Media Team and other relevant staff receive suitable training to enable them to carry out their E-Safety roles effectively and deliver training to other colleagues, as relevant.

● The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

● The Senior Leadership Team will receive regular monitoring reports from the Digital Media Team.

Digital Media Team

● Leads on the responsibility of E-Safety issues.

● 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 network staff.

● Receives reports of E-Safety incidents and creates a log of incidents to inform future e-safety developments.

● Attends relevant meetings/committee of Governors as requested.

● Provides a report regularly to Senior Leadership Team.

Network Manager:

The Network Manager is responsible for ensuring:

● 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 any Local Authority/other relevant body E-Safety Policy/ Guidance that may apply.

● 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 E-Safety technical information in order to effectively carry out their E-Safety role and inform and update others as relevant.

● That the use of the network/ internet/ G-Suite/ remote access/ email iscan be reported regularly monitored in order that any misuse/attempted misuse to the Principal /Designated Senior Leader for 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 Agreement.
- They report any suspected misuse or problem to the Headteacher/ Designated Senior Leader for investigation/action/sanction.
- All digital communications with students/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 understand and follow the E-Safety and acceptable use agreements.
- Students 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 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.

Staff should not contact pupils or parents from their personal mobile phone in or out of school time, or give their mobile phone number to pupils or parents. should be used. This is unless teachers are having to work from home e.g. during the coronavirus pandemic and would need to contact parents/children to check on their wellbeing – in this instant, staff would need to precede any phone call with a blocking system so their phone number is not shared with parents/carers.

- Staff are able to wear wearable technology as long as it does not interfere with teaching and learning across school.

Child Protection/Safeguarding Designated Person:

The Child Protection/Safeguarding Designated Person 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

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's
- Mobile Phones- Students should not be in possession of mobile phones whilst in school. Any student mobile phones found on site will be kept by the office for the duration of the day.
- Wearable technology - Pupils should not be in possession of any wearable tech that has cellular capability (the ability to communicate with other devices inside or outside of school).

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 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.
- Their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 the Digital Media sessions. Other lessons such as PSHE and Collective Worship should have themes and topics in them and should be regularly revisited.

- Key E-Safety messages should be reinforced as part of a planned programme of activities within the Digital Media Curriculum.

- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student 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, social media, the internet and mobile devices.
- In lessons where the internet use is pre-planned, it is best practice that students 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 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:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's online 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 and website
- Parents/Carers evenings/sessions
- Events/ campaigns eg Safer Internet Day
- Circulate and cascade information from the Barnsley and other Yorkshire Safeguarding Children Board and partner agencies

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.
- The school website will provide E-Safety information for the wider community.
- Engaging within Parental Engagement weeks and Parents evenings.

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.
- 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 Digital Media Team/ Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) 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 Digital Media Leader 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 (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring: The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the

relevant people named in the above sections will be effective in carrying out their 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
- All users will have clearly defined access rights to school systems and devices. responsible for the security of their username and password.
- All users will be provided with a username and secure password.
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school 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 incident/security breach to the relevant person, as agreed.
- 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 are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) onto a school device or whilst using the school's systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media should not be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- Other types of media that may exist may only be used for the movement personal data where the user owns the copyright.

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. 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.

- 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.
- Students 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 or change of ownership of the device will be reported.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 students 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images. Please see https://ico.org.uk/media/for-organisations/documents/1136/taking_photos. pdf for more information.
- educational aims, but must follow school policies concerning the sharing, distribution Staff and volunteers are allowed to take digital/video images to support

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 are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Names of students 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 are published on the school website.
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safekeeping 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. 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, 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 or parents/carers (email, chat etc) must be professional in tone and content.
- Students 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 and Local Authorities have a duty of care to provide a safe learning environment for students 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, cyber-bully, discriminate on the grounds of gender, race, religion, sexual orientation or disability 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 students, 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, 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.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

On Induction, all staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner or could potentially bring the teaching profession or school into disrepute a report must be made to the Headteacher/Senior Leader immediately and then the Managing Allegations Procedure and Disciplinary Investigations along with Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The School will encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment. Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate. The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use:

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time. A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accessed inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.
Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

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 "In the Event of Inappropriate Use" above). See flow chart detailed in Appendix A.

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 (Appendix A) for responding to online safety incidents and report immediately to the police.

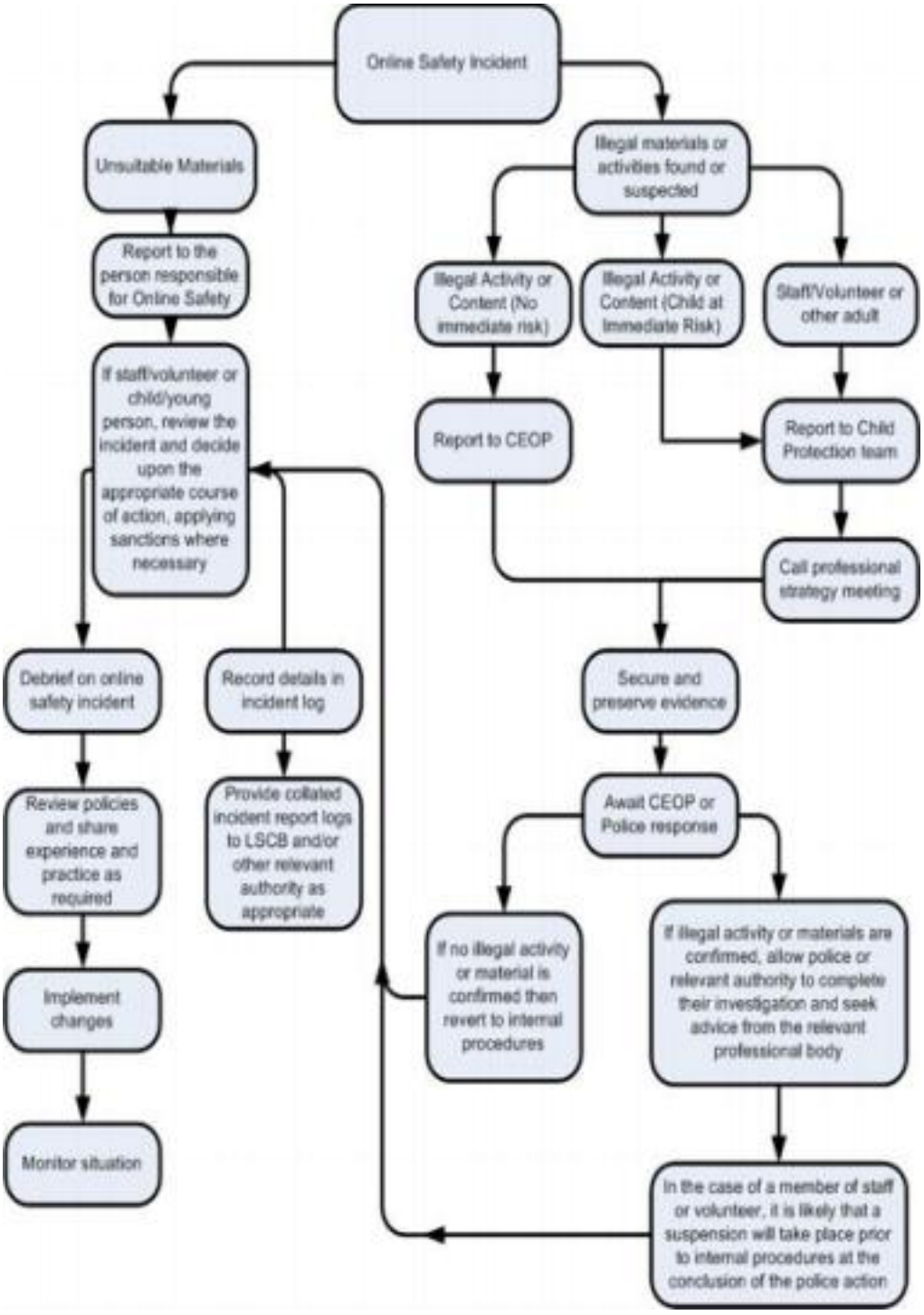
Other Incidents:
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. **In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff/volunteer involved in this investigation 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 Senior Manager for evidence and reference purposes.

Appendix A


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
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
Monitor situation
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