# St. Martin's CE Primary and Nursery School

# E-SAFETY POLICY

## Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

Our school e-safety policy helps to ensure safe and appropriate use of ICT by children at all times as well ensuring that school systems remain secure.

## Development and Monitoring

This e-safety policy has been developed by the Internet Safety Group (360° Group) made up of:

- Lead Governor for Safeguarding
- School Business Manager
- Deputy Safeguarding Lead
- ICT Technician
- Pupils

The school will monitor the impact of the policy using:

- Smoothwall monitoring logs of internet activity (including sites visited)
- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff
- The 360° Tool implemented by the Internet Safety Group

## Scope of the Policy

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

The school 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

### Governing Board

The Governing Board is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Resources Committee receiving regular information about online safety incidents and monitoring reports. The Lead Governor for Health & Safety and Premises on the Governing Board has taken on the role of Online Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings (360 meetings)
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors/Committee meeting

### Head teacher and Senior Leaders:

The Head teacher is responsible 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 School Business Manager.
- The Headteacher and School Business Manager are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (SWGfL's Boost Incident Response Tool).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Online Safety BOOST includes access to unlimited online webinar training – further details are at https://boost.swgfl.org.uk/
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### School Business Manager

The School Business Manager takes the role of Online Safety Lead and is responsible for:

- ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensuring that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance
- ensuring that users may only access the school's networks through a properly enforced password protection policy
- online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- liaising with school IT Technician

- receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments

**ICT Technician:**

The ICT Technician is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet is regularly monitored in order that any misuse / attempted misuse can be reported to the School Business Manager for investigation
- that monitoring systems are implemented and updated as agreed in school / academy 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 school Acceptable Use Statement and the Code of Conduct
- they report any suspected misuse or problem to the Head teacher or School Business Manager.
- Digital communications with pupils 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 school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- designated staff with responsibility for Safeguarding and ICT are informed immediately if content or material deemed inappropriate by the school's policies or Prevent duty are accessed, intentionally or accidentally, and counter measures taken to block further access to such sites.
- they monitor ICT activity in lessons, extra-curricular and extended school activities to ensure they follow the Acceptable Use of Internet
- they are aware of e-safety issues related to the use of mobile phones and hand-held devices and that they monitor their use and implement current school policies with regard to these devices

**Designated Safeguarding Lead / Designated Person / Officer**

Should be trained in Online Safety issues and be aware of the potential for serious 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
- online-bullying

**Online Safety Group (360 Group)**

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production / review / monitoring of the school Online Safety Policy.
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

**Pupils:**

- are expected to use the ICT systems appropriately and in accordance with teacher guidance
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about e-safety campaigns.

Parents and carers will be responsible for:

- endorsing the Acceptable Internet Use Statement.
- supporting the school in promoting good online safety practice
- following guidelines on the appropriate use of digital and video images taken at school events.

**Community Users:**

Community Users who access school ICT systems as part of the Extended School provision will be expected to sign an Acceptable Internet Use Statement before being provided with access to school systems.

## Policy Statements

### Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online 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 programme should be provided as part of ICT/PSHE/literacy lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil Acceptable Internet Use Statement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

### Education – parents / carers

Some 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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site,
- Parents' evenings
- Reference to the SWGfL Boost website

**Education & Training – Staff**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- The school will ensure that all staff are up to date with e-safety procedures. Training will be made available as and when appropriate.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreements.
- The school will ensure all staff are aware of their role under the Prevent duty in assessing the level of risk posed, and preventing exposure or potential draw to, internet sources and social media that promote extremist views or terrorist ideologies
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days

**Training – Governors**

Governors should take part in online safety training, with particular importance for those who are members of the online safety group or those who are Lead Governors for health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / other relevant organisation (e.g. SWGfL).
- 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 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 ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance.
- 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
- Internet access is filtered for all users.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

**Mobile Technologies**

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud-based services such as email and data storage.

- All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The school allows:

| | School Devices | | Personal Devices | | | |
|---|---|---|---|---|---|---|
| | **School owned for single user** | **School owned for multiple users** | **Student owned** | **Staff owned** | **Governor owned** | **Visitor owned** |
| Allowed in school | *Yes* | *Yes* | *No* | *Yes* | *Yes* | *Yes* |
| Network access | *Staff – staff network* | *Staff – staff network*<br>*Pupils – student network* | | *visitor network* | *Staff network* | *visitor network* |

**Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Student's / Pupil's work can only be published with the permission of the parents or carers.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. Parents and carers will be made aware by staff if there are situations where no photos or films can be taken due to there being additional security measures in place for children who are part of the event that parents wish to photograph. In this case, staff will attempt to ensure that they provide photographs that parents are able to download from the school website.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil's parents or carers.

**Data Protection**

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR).
Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school must ensure that**:**

- It has a Data Protection Policy
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.
- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

**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 once it has been transferred or its use is complete.

### Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | *Staff & other adults* | | | *Students / Pupils* | | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to the school / academy | ✓ | | | ✓ | | | ✓ | |
| Use of mobile phones in lessons | | | | | | | | ✓ |
| Use of mobile phones in social time | ✓ | | | | | | | ✓ |
| Taking photos on school devices | ✓ | | | | | | ✓ | |
| Use of school mobile devices e.g. ipads | | | | | | | ✓ | |
| Use of personal email addresses in school or on school network | | | | | | | | ✓ |
| Use of school email for personal emails | | | | | | | | N/A |
| Use of messaging apps (e.g.Dojo) | | | ✓ | | | | | ✓ |
| Use of social media | | | ✓ | | | | | ✓ |
| Use of blogs | | | ✓ | | | | ✓ | |

When using communication technologies the school / academy 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 should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the School Business Manager, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, 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.

**Social Media - Protecting Professional Identity**

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, 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:

- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

**School staff should ensure that:**

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

**Personal Use:**

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- The school permits reasonable and appropriate access to private social media sites

**Monitoring of Public Social Media**

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others

The school’s use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school/academy in online media (newspaper or social media for example) https://boost.swgfl.org.uk/)

### Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

| 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 | |

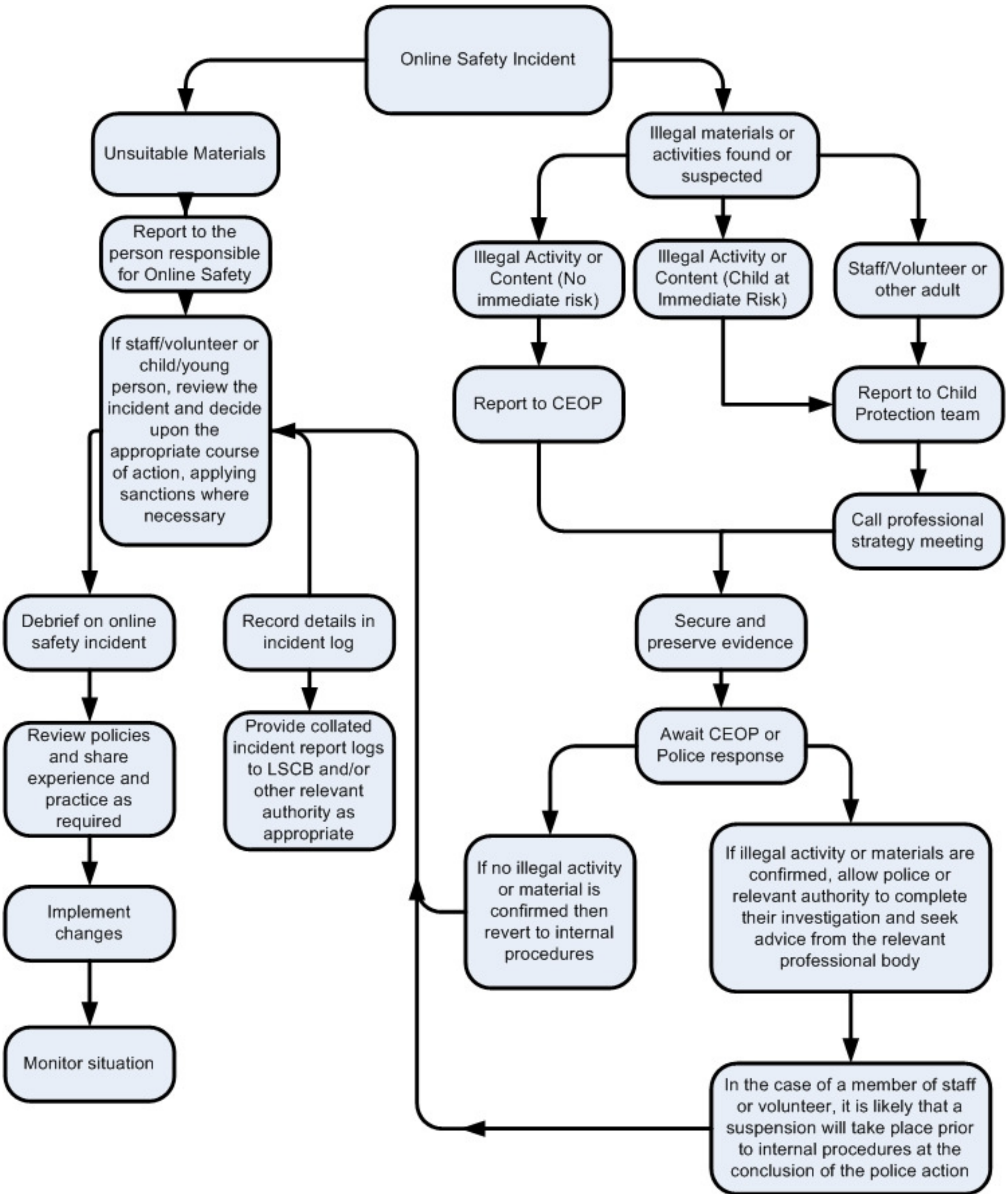
| | | | | | | |
|---|---|---|---|---|---|---|
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | | X | |
| Infringing copyright | | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | | X | |
| On-line gaming (non-educational) | | | | | X | |
| On-line gambling | | | | | X | |
| On-line shopping / commerce | | | X | | | |
| File sharing | | X | | | | |
| Use of social media (School Facebook site) | | | | X | | |
| Use of messaging apps (eg Dojo) | | | | X | | |
| Use of video broadcasting e.g. 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. Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

### Illegal Incidents

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


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

## Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff 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 / Academy Group 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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes

## School / Academy Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Any incidents will be dealt with as soon as possible in a proportionate manner. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

**Acknowledgements**

In order to produce this policy we have referred to the SWGfL School Online Safety Policy Template published in April 2018.

**Policy Review Period: 2 years**

| | |
|---|---|
| **Dates Policy Reviewed:** | **June 2012** |
| | **November 2013** |
| | **18th November 2015 (Nov 15: It was agreed to keep this policy until the planned model Code of Conduct, which will incorporate E-safety, social media use etc, is published by DCC. A standalone Data Protection policy will then be created.)** |
| | **13th April 2016** |
| | **21st November 2018** |
| | |

**Amendments: PREVENT responsibilities included April 2016**