Cantonian High School
Ysgol Uwchradd Cantonian

THE BEST FROM EACH
SUCCESS FOR ALL

E-Safety Policy

June 2018
Revised November 2019

All policies are available on request in large print format or translated into Welsh or community language

Contents

This policy was adopted by Governors on 28 November 2019

Development / Monitoring / Review of this Policy

This E-Safety Policy has been developed by a group of staff made up of:

- Headteacher/Senior Leaders
- E-Safety Coordinator
- Staff – including Teachers, Support Staff, Technical Staff and Network Manager
- Governors

Consultation with the whole school community has taken place.

Schedule for Development / Monitoring / Review

The implementation of this E-Safety Policy will be monitored by:	E-Safety Coordinator
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the E-Safety Policy generated by the monitoring group (which will include anonymous details of E-Safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.	
Should serious E-Safety incidents take place, the following external persons/agencies should be informed:	LA ICT Manager LA Safeguarding Officer Police

The school will monitor the impact of the Policy using:

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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 online 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 of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school.

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. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- attendance at E-Safety Group meetings
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Coordinator.
- 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 flowchart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/other relevant body disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 Headteacher/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 Team will receive regular monitoring reports from the E-Safety Coordinator.

E-Safety Coordinator

- Leads the E-Safety Group.
- 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.
- Lliaises 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 the E-Saftey Governor to discuss current issues.
- Attends relevant meetings/committees of Governors.
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff

The Network Manager is responsible for ensuring:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- 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.
- The school's curriculum internet filtering is regularly updated.
- 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.
- The use of the network/email is regularly monitored in order that any misuse/ attempted misuse can be reported to the Headteacher/Senior Leader or E-Safety Coordinator for investigation/action/sanction
- Monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of 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 the Headteacher/Senior Leader or E-Safety Coordinator for investigation/action/sanction.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the E-Safety Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Safeguarding 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
- Online-bullying

E-Safety Group

The E-Safety Group 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. Depending on the size or structure of the school, this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body. Members of the E-Safety Group will assist the E-Safety Coordinator with:

- The production/review/monitoring of the school E-Safety Policy/documents.
- Mapping and reviewing the E-Safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- Regularly and proactively reviewing incident logs.
- Consulting stakeholders – including parents/carers and the pupils about the E-Safety provision.
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- 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 E-Safety practice when using digital technologies out of school and realise that the school's '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 / Learning Platform 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 / Learning Platform and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / Learning Platform 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 – 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 / digital literacy is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

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

- A planned E-Safety curriculum should be provided as part of ICT & Computing / PHSE / 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
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be 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
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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 providing adequate advance notice to allow for filters to update.

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 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, web site, Learning Platform
- Parents' / Carers' evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

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 online safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents
- Supporting community groups e.g. 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.

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.

- It is expected that some staff will identify E-Safety as a training need within the performance management process.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / 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 E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or 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 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:

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- 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 internet access of "guests" (e.g. trainee teachers, supply teachers, visitors)
- An agreed policy is in place regarding the extent of personal use that users (staff / 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.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned / provided or personally owned and might include: smartphone, tablet, notebook / 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 the school's learning platform and other 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 mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's E-Safety education programme.

The school Acceptable Use Agreements for staff, pupils and parents / carers will give consideration to the use of mobile technologies

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- 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 pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

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

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones brought to the school	X				X			
Use of mobile phones in lessons		X						X
Use of mobile phones in social time	X				X			
Taking photos on mobile phones				X				X
Use of other mobile devices e.g. tablets, gaming devices	X					X		
Use of personal email addresses in school or on school network		X						X
Use of school email for personal emails				X				X
Use of messaging apps		X						X
Use of social media			X					X
Use of blogs	X					X		

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 pupils or parents / carers (email, social media, chat, blogs, VLE 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.
- 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 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, 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
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

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 according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety Group to ensure compliance with the school policies.

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 following is not permited:

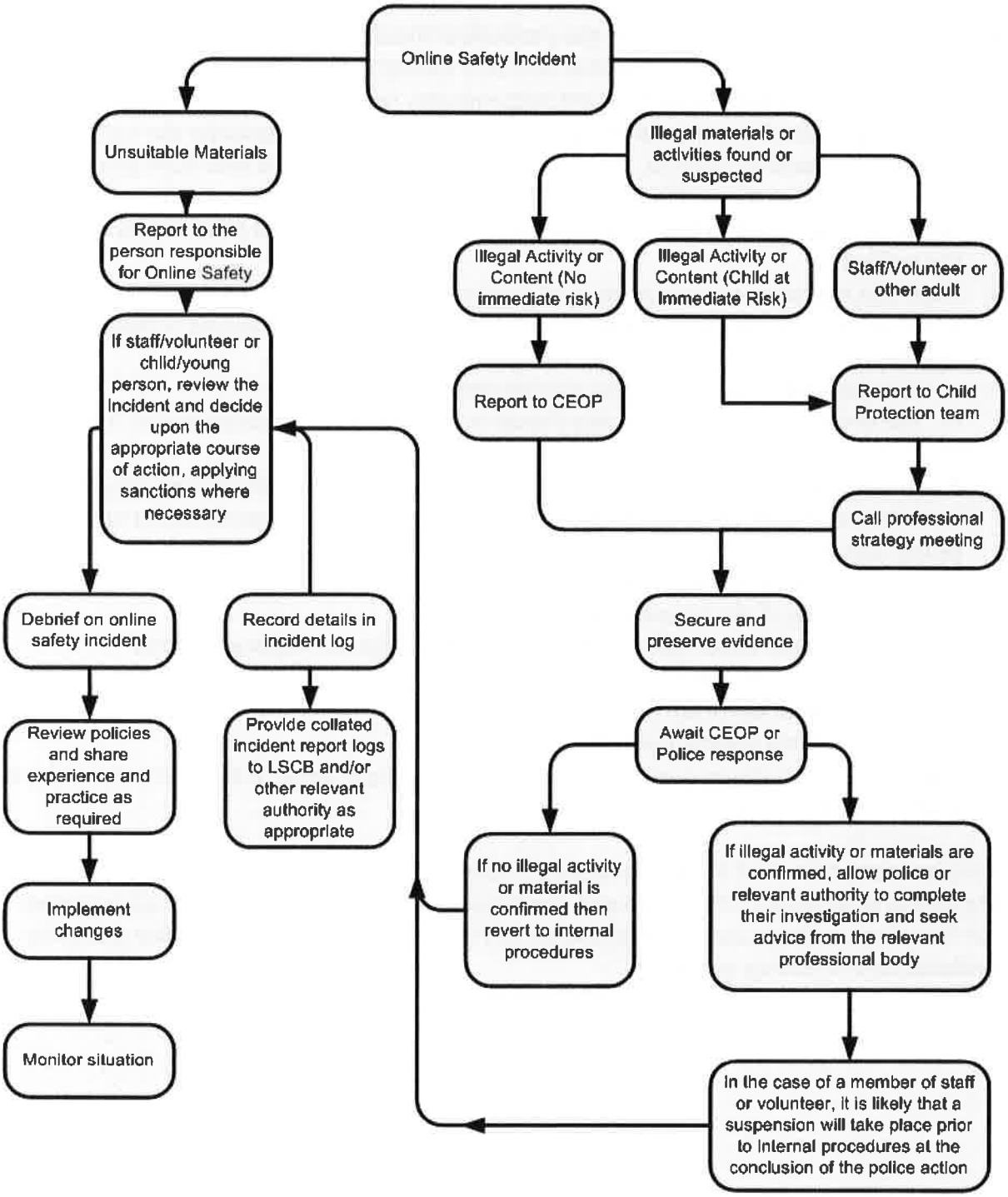
- Child sexual abuse images –The making, production or distribution of indecent images of children – contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children – contrary to the Sexual Offences Act 2003
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) – contrary to the Criminal Justice and Immigration Act 2008
- 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
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- 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
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- On-line gaming (non-educational)
- On-line gambling
- On-line shopping/commerce

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 website(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 for responding to E-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 involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- 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 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.

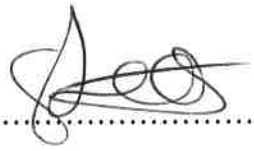
School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re: filtering/security etc.	Inform parents/carers	Removal of network / internet access rights	Warning	Further sanction, e.g. detention
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised/inappropriate use of mobile phone/ digital camera/other mobile device	X							X	X
Unauthorised /inappropriate use of social media/ messaging apps/personal email	X							X	
Unauthorised downloading or uploading of files	X						X		X
Allowing others to access school network by sharing username and passwords		X					X		X
Attempting to access or accessing the school network, using another/pupil's account		X						X	
Attempting to access or accessing the school network, using the account of a member of staff			X				X		X
Corrupting or destroying the data of other users		X			X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			X
Continued infringements of the above, following previous warnings or sanctions			X				X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						X
Using proxy sites or other means to subvert the school's 's filtering system			X		X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X							
Deliberately accessing or trying to access offensive or pornographic material			X				X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X						X

Policy Review

This policy will be reviewed annually.

Agreed by Headteacher: 

Agreed by Chair of Governors: 

Date of Issue: 28.11.19

Date for Review: October 2020