Online Safety Policy

Approval Date: **March 2019**

Review Date: **September 2027**

Headteacher: T Emberson

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of:

- HT,
- Online Safety co-ordinator,
- and support from JSPC.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Headteacher on:	27th February 2019
The implementation of this Online Safety policy will be monitored by the:	The Headteacher, Governing Body and the Online Safety Co-ordinator
Monitoring will take place at regular intervals:	Once a year
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	September 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer / Police (as appropriate)

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- 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 students / 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 Online Safety incidents covered by this policy, which may

take place outside of the school, but are 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 (see appendix for template policy). 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, Andrew Eley, has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Attendance at Online Safety Group meetings
- Reporting incidents 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 online safety will be delegated to the Online Safety Co-ordinator
- 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 online safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that the Online Safety Co-ordinator 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 Senior Leadership Team will be alerted of serious incidents reports from the Online Safety Co-ordinator.

Online Safety Co-ordinator

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Headteacher
- Liaises with JSPC (ICT Outside Contractor)
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets, as needed, with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings as needed
- Reports as needed to Senior Leadership Team.

JSPC (ICT Outside Contractor)

JSPC is responsible for ensuring:

- **That the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **That the *school* meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.**
- **That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed once a year**
- *The school's filtering solution allows for deep packet inspection of all communications, providing detailed monitoring and reporting, and the ability to block keyword searches in search engines. The product is Surfprotect Quantum, provided by EXA Broadband.*
- 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 / Learning Platform / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- **They have an up to date awareness of the current school Online 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 / Online Safety Co-ordinator 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***
- Online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies.

Designated Safeguarding Lead

Should be trained in Online 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.

Pupils:

- **Are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Agreement (Older Children & Younger Children Agreements)**
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be taught throughout the curriculum about the use of mobile devices out of school/at home and digital cameras. Pupils 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 Online 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 termly learning conferences, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online 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.

Community Users

Community Users who access school systems / website 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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online 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 online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online 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 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*
- *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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (JSPC) can temporarily*

remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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*
- *Termly learning conferences*
- *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 (see appendix for further links / resources).*

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online 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*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community.*

Education & Training – Staff / Volunteers

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

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.** Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and**

Acceptable Use Agreements. Online Safety BOOST includes an array of presentations and resources that can be presented to new staff

- *It is expected that some staff will identify online safety as a training need within the performance management process*
- *The Online Safety Co-ordinator (or other nominated person) 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 Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days*
- *The Online Safety Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.* Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff. It includes presenter notes to make it easy to confidently cascade to all staff.

Training – Governors

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

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL)
- Participation in school training / information sessions for staff or parents, including attendance at assembly and visiting classes.

Technical – infrastructure / equipment, filtering and monitoring

The school has a managed ICT service provided by JSPC, who carry out all the online safety measures. JSPC is fully aware of the school Online Safety Policy / Acceptable Use Agreements.

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 online safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**

- **All users will have clearly defined access rights to school technical systems and devices**
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- JSPC is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- **Internet access is filtered for all users.** 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. Staff request changes to JSPC (during the weekly visit to the school by JSPC)
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- *The school has provided enhanced / differentiated user-level filtering*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement*
- *Users should report any actual / potential technical incident / security breach to the relevant person, via CPOMS*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- There is provision of temporary access of "guests" (e.g. supply teachers) onto the school systems via a specific user account that has access to one folder on the shared drive
- It is not possible for standard users to install programmes on school devices

The use of removable media is permitted on school devices, as long as any personal or sensitive information is encrypted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. See School Personal Data Advice and Guidance for further detail.

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. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Use of digital and video images

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

- **When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites**
- **Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press (included in the initial pupil enrolment form)**
- 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 parents or carers.

Data Protection

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 paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (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 (NB including Academies, which were previously exempt) 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. Data is sent over the school's e-mail service within the same domain, which is encrypted via TLS, or transferred through an encrypted memory stick.

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 (many memory sticks / cards and other mobile devices cannot be password protected)
- **The device must offer approved virus and malware checking software**
- **The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

The Personal Data Advice and Guidance in the appendix provides more detailed information on the school's responsibilities and on good practice.

Communications

When using communication technologies, the school considers the following as good practice:

- Staff and pupils should 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 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.** (Online Safety BOOST includes an anonymous reporting app Whisper)
- **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 online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, academies, 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 / MAT 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 Online Safety BOOST includes unlimited webinar training on this subject)
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority / MAT
- 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 accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, 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

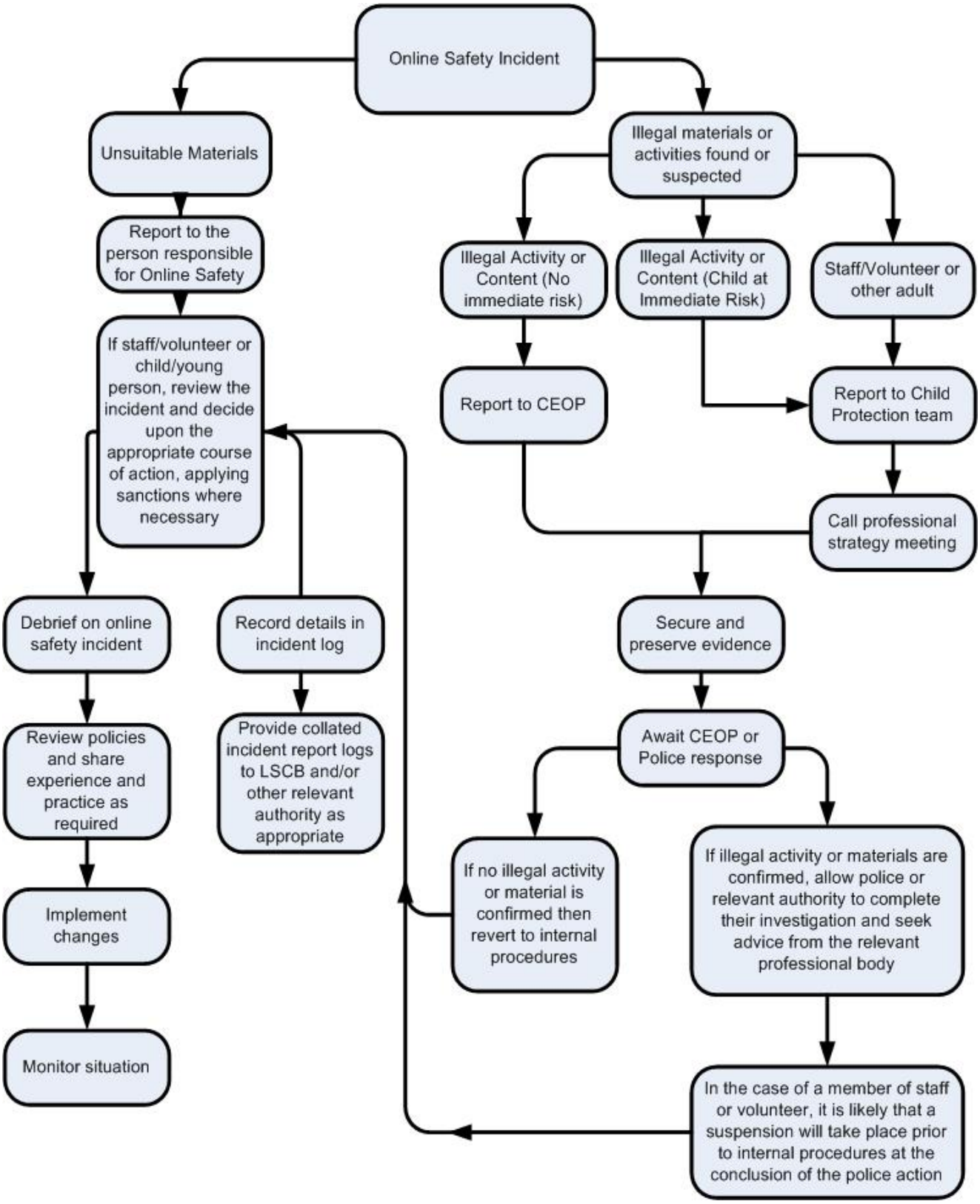
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites.*

Monitoring of Public Social Media

- The school should effectively respond to social media comments brought to its attention made by others according to a defined policy or process
- Online Safety BOOST includes Reputation Alerts that highlight any reference to the school in online media (newspaper or social media for example).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) 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 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 incident log (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.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

SWGfL Online Safety Policy Templates

https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/

Previous Online Safety Policy Approved October 2017