Online Safety Policy

Reviewed by: Mike Nelson (adopted from SWGL model policy)

Governor responsibility: FGB

Date of Policy: Sep 2023 **Review Date:** Sep 2024

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 the 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 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 Quality and Outcomes Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body will take on the role of Online Safety Governor, which is part of the Safeguarding Lead role.

The role of the Online Safety Governor will include:

- periodic meetings with the Online Safety Co-ordinator
- periodic monitoring of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g online safety education provision and staff training is taking place as intended)

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 other members 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. (see flow chart on dealing with online safety incidents)
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online 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 online 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 Online Safety Co-ordinator.

Designated Safeguarding Lead / Designated Person / Officer

- have a leading role in establishing and reviewing the school online safety policies / documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- provides training and advice for staff
- liaises with the Local Authority, technical, pastoral and support staff

This individual 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
- cyber-bullying

Welfare Manager role

- takes day to day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Safeguarding Governor to discuss current issues, review (anonymised) incident and if possible, filtering and monitoring logs.
- attends relevant meeting / committee of Governors reports regularly to Senior Leadership Team
- reports regularly to the Senior Leadership Team

ICT Support:

The ICT Support is responsible for ensuring:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any Local Authority Guidance that may apply.

- There is clear, safe, and managed control of user access to networks and devices
- The use of technology is regularly and effectively monitored in order that any misue/attempted misuse can be report to the online safety coordinator for investigation and action
- the filtering procedures are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- monitoring software / systems are implemented and updated as agreed in school procedures

Curriculum Leads

Curriculum leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through

- a discrete programme
- PHSE and SRE Programmes
- A mapped cross-curricular programme
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities e.g Safer Internet Day and Anti Bullying week

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the Staff Acceptable Use agreement (AUA)
- they immediately report any suspected misuse or problem to the Online Safety Coordinator for investigation / action, in line with school safeguarding procedures.
- 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 pupils understand and follow the Online Safety Policy and acceptable use policies
- they supervise and 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
- where lessons take place using live-streaming or video conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- Have a zero tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Designated Safeguarding Lead / Designated Person / Officer

This individual 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
- cyber-bullying

Pupils:

Where appropriate, the following points will apply:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- 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

The school will take every opportunity to help parents understand these issues through

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learner's acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permission concerning digital images, cloud services etc.
- parents/carers evenings, newsletters, website, social media and information about national/local online safety campaigns and literatures And information about national / local online safety campaigns / literature.

Parent and carers will be encouraged to support the school in:

- reinforcing the online safety message provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)

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

Online Safety Education Programme

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 for all years groups matched against nationally agreed framework e.g Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g PHSE; SRE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g safer internet day and anti-bullying week.
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.
- Key online 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 materials / 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 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

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

- Regular communication, awareness-raising and engagement on online safety issues, Curriculum activities and reporting routes

- Letters, newsletters, website Parents / Carers evenings, Class Dojo
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

All staff will 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.
- The training will be an integral part of the school's annual safeguarding and data protection training for all 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. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- The DSL will receive regular updates through attendance at external training events (eg from 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 Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee 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 / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents, this may include attendance at assemblies / lessons.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- the school filtering is agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours

- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content.
- there is a clear process in place to deal with requests for filtering changes.

Monitoring

The school has monitoring systems in place to protect the school, systems, and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders

Technical Security

The 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
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies are kept in the cloud.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Support and will be reviewed, at least annually
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security

- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by IT Support who will keep an up-to-date record of users and their usernames All Pupils will be provided with a class username and password.
- The "administrator" passwords for the school ICT system, used by the ICT Support must also be available to the Headteacher, School Business Manager or other nominated senior leader and kept in the school safe.
- ICT Support 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.
- 'Every' system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts, which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school, (please see the school's remote learning policy).
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

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

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*Yes*	*Yes*	*Yes*
No network access				*No*	*No*	*No*

Mobile Phone Policy (pupils)

Any mobile phones brought into the school are done so at the pupil's own risk.

The aims of the mobile phone policy are:

- To ensure that all classrooms are learning spaces, that avoids distractions from mobile phones
- To reduce confrontations between staff and pupils when challenged about mobile phone use
- To make sure that pupils are not walking around whilst using mobile devices and therefore reducing safety hazards

Mobile phones can be used in the following areas only:

- In supervised classrooms for purposes instructed by the teacher
- In an emergency, with express permission from a member of staff

Mobile phones CANNOT be used in other areas of the school.

Consequences for pupils not following the above policy:

- Staff will confiscate the mobile phone and it will be held by the class teacher
- First offence – the mobile phone will be returned to the pupil at the end of the school day
- Second offence – parents will need to come to school and collect the mobile phone. The confiscated mobile phone will be kept in a locked safe until it is collected
- Third offence – the pupils will be put on a mobile phone ban and a letter/email will be sent home to the parent/carer
- If it is proved that a pupil has used his/her phone to bully or intimidate another person, the phone will be confiscated and returned only to a parent/carer. The school will then decide on the appropriateness of that pupil having a mobile phone in school following such an incident.
- Any future misuse of the mobile phone will return in a total ban for that pupil on having a mobile phone in school. The ban will continue until it is certain that the pupil will in future use the phone in an appropriate manner at all times

Social Media

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
- Guidance for learners, parents and carers

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
- they act as positive role models in their use of social media

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

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, 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

- 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
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the complaints procedure.
- The school's use of social media for professional purposes will be checked regularly by the DSL to ensure compliance with the school policies.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff will 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.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 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.
- 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 the Online Safety Policy
- 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.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Class Dojo
- Online newsletters

The school website is managed/hosted by Brave Creative (Heart Internet). The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

General Data Protection Regulations

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations

The school:

- has a General Data Protection Regulation Policy
- implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records
- had paid the appropriate fee for information commissioner's office (ICO) and included details of the Data Protection Officer (DPO)
- has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- has an "information asset register" in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this, personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- It provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- Has procedures in place to deal with individual right of the data subject, e.g Subject Access requests.
- Data protection impact assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote solutions, or entering into a relationship with a new supplier.
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom
- has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- understands how to share data lawfully and safely with other relevant data controllers
- reports any relevant breaches to the information commissioner within 72 hours of becoming aware of the breach in accordance with the UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling request

under the individuals rights, will receive training appropriate for their function as well as the core training provided to all staff

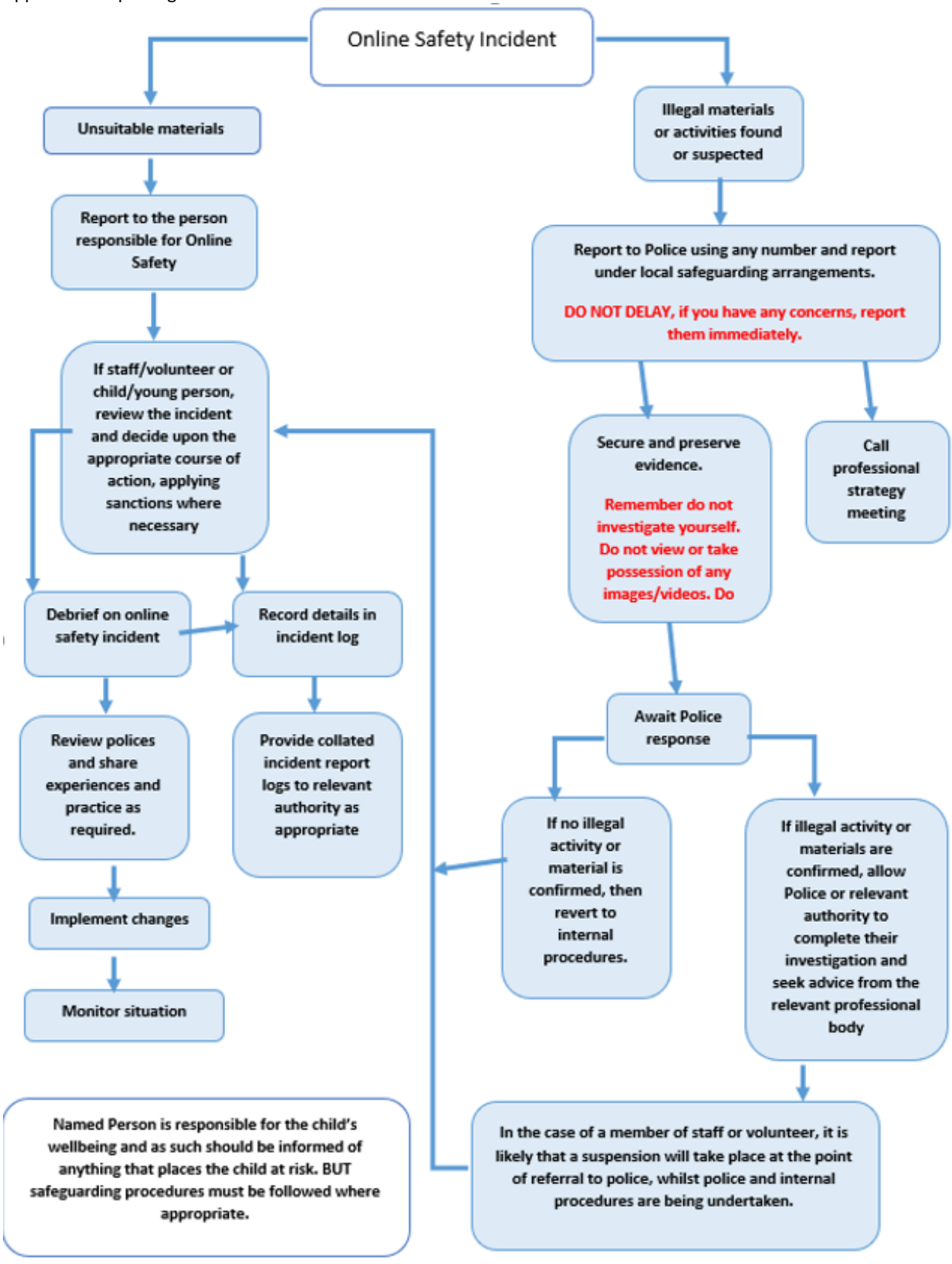
Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it onto in school
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted or password protected
- Will not transfer any school personal data to personal devices except as in line with school policy
- Access personal data sources and records 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

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 be protected by up to date 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

Appendix – Reporting Process



LSCB = Local Safeguard Children Board (01733 864170)

CEOP = Child Exploitation Online Protection (https://www.ceop.police.uk/ceop-reporting/)

Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this 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
    - 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
- offences under the Computer Misuse Act
- 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 and lead to suspense/dismal dependant on level of misuse.