ROUNDHAY SCHOOL

EST. 1903

Policy name: **Online Safety Policy**

Author: **Steve Palmer & Rob Wilks**

Governor committee: **Pastoral & Staffing**

To be approved by: **Committee**

Date approved: **21 May 2019**

Review date: **Summer Term 2022**

Applicable to

PRIMARY CAMPUS

SECONDARY CAMPUS

SIXTH FORM

Development / Monitoring / Review of this Policy

This online safety policy has been developed by a working group made up of:

- Senior Leaders, including the Director of Operations
- Staff – including the Curriculum Leader of Computing and the ICT Systems Manager
- Governors

Consultation with parents and students/pupils has taken place through ongoing dialogue and pupil/parent voice.
The policy has been constructed with reference to the South West Grid for Learning model.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Pastoral & Staffing committee of the governing body on:	*21 May 2019*
The implementation of this online safety policy will be monitored by the:	*Director of Operations, and the Senior Leadership Teams at both campuses*
Monitoring will take place at regular intervals:	*Every Year*
The relevant committee of the Governing Body will receive a report on the implementation of the online safety policy (including anonymous details of online safety incidents) at regular intervals:	*Termly, via the relevant committee and/or specific impact meetings convened*
The Online safety Policy will be reviewed tri-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:	*Summer Term 2022*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*CEOP, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents (CPOMS)*
- *Logs of data protection incidents and DPO reports*
- *Monitoring logs of internet activity (including sites visited)*
- *Logs and notifications of key word and phrase monitoring*

Scope of the Policy

This policy applies to all members of the school community (including staff, students/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 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 cyber-bullying, or other online 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 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.
The designated Safeguarding governor will also:

- convene impact meetings with the relevant staff in school (Director of Operations, Designated Safeguarding Lead, Curriculum Leader for Computing and ICT Systems Manager) *to enable them to*
- monitor the implementation of this policy, and the incident and monitoring logs *which will result in*
- reporting to the relevant Governors

Headteacher and Senior Leadership Team

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 Director of Operations and the Designated Safeguarding Lead.

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 (see enclosed flow chart on dealing with online safety incidents and the relevant HR and disciplinary procedures).

The Headteacher and Senior Leadership Team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal 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 Director of Operations and Designated Safeguarding Lead.

Online Safety Leads

The Designated Safeguarding Lead has the following responsibilities:

- takes day to day responsibility for ensuring online safety issues are responded to promptly and appropriately
- ensures incidents and actions are recorded in CPOMS
- coordinates training and advice for staff about responding to safeguarding concerns related to online safety
- liaises with the Local Authority

They should also 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

The Director of Operations has the following responsibilities:

- has a leading role in establishing and reviewing the school online safety policies / documents
- coordinates training and advice for staff around the school systems around online safety
- liaises with school technical staff
- receives summary reports of online safety incidents and ensures a log is maintained to inform future developments
- meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering logs

Together they will also:

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- attends relevant Governor meetings and reports regularly to Senior Leadership Team

ICT Systems Manager

The ICT Systems Manager will ensure:

- 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 policy/guidance

- that users may only access the networks and devices through a properly enforced password protection policy which enforces an appropriate level of complexity and, for staff accounts, requires passwords to be changed regularly
- the filtering policy, is applied and updated on a regular basis and that its implementation can also be managed by the senior technician
- 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, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to a senior leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

All 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, including the use of social media
- they have read and understand the Staff Acceptable Use Policy printed in the staff handbook
- they report any suspected misuse or problem to a senior leader for investigation / action / sanction
- all digital communications with students/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 and acceptable use policies
- students/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 students/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

Students/pupils

- are responsible for using the *school* digital technology systems in accordance with the Student/Pupil Acceptable Use Policy as display in classrooms (primary only) or set out in the pupil planner (secondary only)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 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 parents' evenings, 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 and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

The necessary policy and guidance will be shared with parents via the school website and/or via the pupil planner as appropriate. The school will also signpost parents to relevant resources (online and/or print) to support them.

POLICY STATEMENTS

Education and Training

Students/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students/pupils to take a responsible approach. The education of students/pupils in online safety 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 and PHSE 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
- Students/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.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should be helped to understand the need for the student/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 students/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 students/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, students 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 ICT Systems Manager and/or the ICT Technicians 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.

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 on-line 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 methods such as:

- Curriculum activities
- Letters, newsletters and the school website
- Parents sessions
- High profile events/campaigns (e.g. Safer Internet Day)
- Reference to the relevant web sites/publications
  For example www.swgfl.org.uk, www.saferinternet.org.uk, http://www.childnet.com/parents-and-carers

Wider Community

The school will provide opportunities for the wider 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 the wider family as well as parents
- The school website providing online safety information for the wider community

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:

- online safety training will form part of the regular safeguarding training for staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.

- 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.
- Nominated staff will receive regular updates through attendance at external training events (e.g. from South West Grid for Learning, local authority or 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
- The Online Safety Leads will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub committee or group involved in technology, online safety, health and safety and/or 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

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 online safety responsibilities.

The responsibilities include:
- School 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
- All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password . Reception and KS1 students are provided a class login
- The ICT Systems Manager will ensure an up to date record of users and their usernames is maintained.
- The “administrator” passwords for the school ICT system, used by the ICT Systems Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- The ICT Systems Manager 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.
- The school has enhanced, differentiated user-level Web filtering. Content is filtered based on Key Stage with older students given more access to media sites such as YouTube. Staff are given even greater access.
- 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 which must be auditable.
- The ICT technicians team 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. Web traffic is monitored and logged by the Internet filter system and key word/phrase monitoring is in place to identify safeguarding concerns.
- When a member of the ICT technicians team identifies a concern this is logged within CPOMS. When this concern is urgent they make immediate contact with a member of the safeguarding team.
- 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 systems or data. These are tested regularly. The school infrastructure and workstations are protected by up to date virus software.
- All "guests" (eg trainee teachers, supply teachers, visitors) with access to school systems are required to accept the school's Acceptable Use Agreements.
- Systems are in place to verify downloaded files and protect the network in case of malicious attack. Permission to install programmes on school devices is restricted.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom.

The school has a separate Bring Your Own Device (BYOD) in place which addresses some key issues.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the GDPR (General Data Protection Regulation) principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's filtering systems while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students/pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation, and in compliance with the school's Data Protection Policy. All staff receive data protection training, both through the induction programme and ongoing staff training, and are made aware of their responsibilities. Guidance is provided in the staff handbook and reinforced by regular reminders in the staff newsletter.

Guidance to staff includes:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Avoid leaving paper copies lying around - keep sensitive information locked away.
- Always shred documents that contain personal data.
- Do not keep sensitive information in markbooks - colour code or markup instead so no-one else can understand it
- Do not take personal data (beyond basic markbook data) offsite without explicit permission
- Never share their login details with anyone (including other staff) as they have different permission
- Always lock their computer when they are not using it
- Think carefully about where they store files and who will be able to access them in that location
- Avoid storing data on your PC - store it on the network itself
- Encrypyt/password protect files containing any sensitive data
- Avoid downloading or storing any personal data to a personal device
- Use the remote desktop. This can be from a personal device as the data does not leave the school network
- Use the OneDrive storage facility in their school email to move files. Files can be edited in your browser
- If they wish to use an app to store data on a device it needs authorizing and recording by SPA or LFO
- Avoid using USB keys where possible, and ensure any that are utilised are encrypyed/password protected
- Only ever use their school email to communicate data about pupils
- Avoid blanket emails to all staff - send data only to those who need it
- Think carefully when forwarding an email or copying someone in - should they see the whole trail?
- Never use names in the subject line
- Don't include sensitive data in emails - place in a secure location (network/OneDrive) and share
- If they must attach a data file then encrypt it

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/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 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.
- 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 or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims as set out in the school's Data Protection Policy. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission.
- Permission to use photographs for purpose beyond educational assessment is sought from parents/carers and/or students (as required dependent on the age of the student/pupil) and photographs may only be used if the necessary consent has been received for the purpose for which they will be used.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Communications

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. When in school, or on school systems (e.g. by remote access), staff and students/pupils should therefore use only the school email service to communicate with others.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers must be professional in tone and content. These communications may only take place on official and monitored school accounts. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students/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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, 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 therefore provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

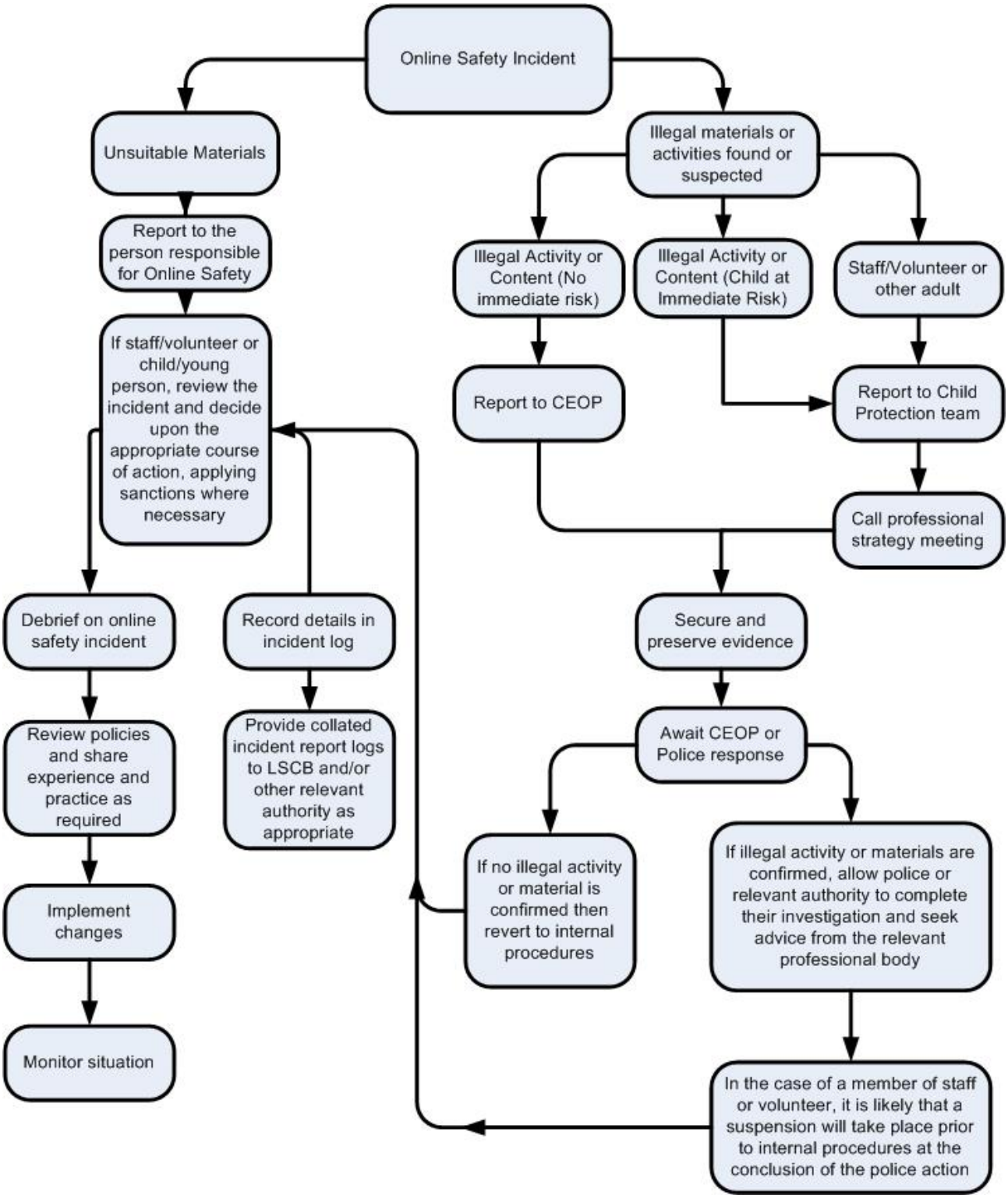
School staff should ensure that:

- No reference should be made in social media to students/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.

The school's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 / 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).

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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