Online Safety and Social Media Policy

Key Information

Title	Online Safety and Social Media Policy	
Prepared By	Mr Adrian Foley (Head of Computer Science)	09/06/2023
Checked By	Mrs Karen Tyler (Data Manager)	21/06/2023
Approved By	Governors' Christian Vision Committee	
Version	V01.02	
Document Update	June 2024	

Version History

Version	Date	Amendments
V01.00	June 2021	Approved by Governors
V01.01	June 2022	BYOD information added
V01.02	June 2023	Artificial Intelligence Language Models such as ChatGPT Usage

Schedule for Review

This Online Safety and Social Media Policy was approved by the Governors in:	June 2023
The implementation of this Online Safety and Social Media Policy will be monitored by the:	Head of Computer Science Senior Leadership Team
Monitoring will take place at regular intervals:	Twice a year
The Governors will receive a report on the implementation of the Online Safety and Social Media Policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Twice a year
The Online Safety and Social Media 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:	June 2024
Should serious Online Safety incidents take place the following external persons/agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police, NCA (National Crime Agency)

The school will monitor the impact of the policy using:

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

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents, carers and visitors) 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 the Headteacher, to such extent as is reasonable, to regulate the behaviour of students 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 for Excellence 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.

The policy should be read in conjunction with the following policies;

- Behaviour for Excellence
- IT Acceptable Use Policy (Student)
- IT Acceptable Use Policy (Staff)
- Anti-Bullying Policy
- Equality Objectives
- Spiritual, Moral, Social and Cultural Development Policy
- Staff Code of Conduct
- Child Protection and Safeguarding Policy
- Data Protection Policy

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 and Social Media 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 has taken on the role of Data and E-Safety Governor. This role will include:

- regular meetings with the Head of Computing;
- regular monitoring of Online Safety incident logs;
- regular monitoring of filtering logs;
- reporting to the relevant Governors' meeting.

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 Head of Computing, the Director of Pastoral Care and the Heads of Year;
- The Headteacher, the Director of Pastoral Care and the Assistant Head (Teaching and Learning) are 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 included in "Responding to incidents of misuse" below, and relevant Local Authority advice);
- The Headteacher and Senior Leaders are responsible for ensuring that the Head of Computing 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 and 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 to support those colleagues who take on important monitoring roles;
- The Senior Leadership Team will receive regular monitoring reports from the Head of Computing.

Head of Computer Science

The Head of Computing:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies and 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 Local Authority/relevant body;
- liaises with school technical staff;
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments;
- meets regularly with the Data and E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs;
- attends relevant meetings of Governors;
- reports regularly to the Senior Leadership Team.

Network Manager

The Network Manager 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 Guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- the filtering policy is 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;
- that the use of the network, internet, remote access and emails are regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher/Head of Computing for action;
- that monitoring software is implemented and updated as agreed in school policies.

Teaching and Support Staff

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 have read, understood and signed the IT Acceptable Use Policy (Staff);
- they report any suspected misuse or problems to the Headteacher, Director of Pastoral Care or Head of Computing for action;

- all digital communications with students, parents and 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 understand and follow the Online Safety and IT Acceptable Use (Students) policies;
- students 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 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.

Designated Safeguarding Lead

The DSL should be trained in Online Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data;
- access to illegal and/or inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying;
- sharing sexual images;
- upskirting.

Students

Students:

- are responsible for using the school digital technology systems in accordance with the IT Acceptable Use Policy (Students);
- 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;
- should know and understand policies on the taking and use of images and on cyber-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 and Social Media Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help

parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and 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 records;
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 the Computer Science and PSHE curriculum. This should be regularly revisited to provide updated information.
- In Computer Science at Key Sage 3, one full term is dedicated to educating students in online safety issues that are relevant to their age.
- At Key Stage 4, relevant online safety information is provided to the students through focussed PSHE sessions.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities. Annually, during or near to the relevant Internet Safety Week, assemblies for all year groups will take place and tutorial activities provided by the Head of Computing.
- Students 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the IT Acceptable Use Policy (Students) 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 should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches should be reported to the Network Manager and/or Head of Computing.
- Where students can 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 Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be agreed with the Head of Computing in advance, with apparent reasons for the need.

Education – Special Education Needs

Students who have Special Educational Needs are in truth more vulnerable to deceptive messages offering friendship or to opening dialogue on topics of mutual interest. This could include issues surrounding grooming, sexting and cyber-bullying.

For example, those students with autistic spectrum traits can take messages very literally and could be persuaded to act upon them. These students are likely to need:

- additional advice on safe behaviours;
- to be reminded what they should never disclose to others online;
- increased supervision which could include, for example, guidance that before entering dialogue with anyone new, they should always consult a trusted adult.

Education – Parents and 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 and regulation of their child's on-line behaviour. 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, the school website
- Parents evenings
- Specific Age-Related Parent assemblies
- High profile events/campaigns, e.g. Safer Internet Day
- Reference to relevant web sites / publications such as
  - www.swgfl.org.uk
  - www.saferinternet.org.uk/
  - http://www.childnet.com/parents-and-carers

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 through Hot Spots. This will be regularly updated and reinforced.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety and Social Media Policy and IT Acceptable Use (Staff) agreement.
- **All members of staff (Including Governors)** should be made aware (through relevant training) that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Where necessary and if appropriate the Head of Computing (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/ other relevant organisations like the National Crime Agency) and by reviewing guidance documents released by the relevant organisations.
- This Online Safety and Social Media Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Head of Computing (or other nominated person) will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in Online Safety training and awareness sessions, with importance for those who are members of any subcommittee involved in technology, online safety, health and safety and child protection. This may be offered in several ways:

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

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their 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.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every Term. (See Technical – Password section).

- The 'administrator' passwords for the school ICT system, used by the Network Manager (or another person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The Network 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. Content lists are regularly updated, and internet use is logged and regularly monitored.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users, i.e. staff, students, etc).
- 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 IT Acceptable Use policies for staff and students.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the Network Manager or Head of Computing.
- 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" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Technical – Security and Management of Information Systems

- The Network Manager will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used on the school computer system without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Head of Computing/Network Manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices.

Technical – Password

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.

- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.
- We require staff and students to use STRONG passwords for access into our system.
- We require staff and students to change their passwords every term.

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. This has led to users bringing their own technologies in order to provide a greater freedom of choice and usability.

Staff and sixth form students may use their own personal devices (pcs, laptops, tablets, mobile phones etc) to access the school network, school emails and cloud based apps used by the school, provided they adhere to the following guidelines:

- The personal device must have appropriate security software installed;
- Personal PCs and laptops must be password protected with a strong password (ie at least eight characters and having at least one lower case letter, one upper case letter, one digit and one special character);
- Mobile phones must require facial recognition, a fingerprint, a pattern or a passcode to be entered in order to access emails or apps containing personal data on them;
- When on the school site, staff and students must use the school WiFi for school related work. The Wi-Fi password must not be shared with anyone else. Staff and students must not access inappropriate or illegal content and should remember that the use of personal devices connected to the WiFi is monitored;
- The device must not be left unattended whilst accessing the school network, school emails or cloud based apps containing personal data about members of the school community;
- Personal data MUST NOT be downloaded from the school network onto personal devices;
- Personal data MUST NOT be downloaded onto personal devices from cloud based apps.

Students in Years 7 to 11 may not use their own devices on the school site.

Please note that inappropriate use of personal devices could result in a Data Protection breach.

Artificial Intelligence Language Models such as ChatGPT Usage

The purpose of this section is to establish guidelines for using artificial intelligence language models (AILMs), such as ChatGPT, Bard, Bing or other similar tools by members of staff and students. There is a need to ensure that the use of AI is ethical, lawful, and in compliance with all applicable laws, regulations and school policies.

Members of staff are authorised to use AILMs for work-related purposes, to gather knowledge of how they work and where students may use them. Students are not allowed to use AILMs for school related projects, homework or any school related tasks.

The use of AILMs has inherent risks that all members of staff should be aware of. These risks include, but are not limited to:

- **Copyright:** Members of staff must adhere to copyright laws when utilising AILMs. It is prohibited to use AILMs to generate content that infringes upon the intellectual property rights of others, including all copyrighted material.

- **Confidentiality:** Confidential information must not be entered into an AILM tool as information may enter the public domain. Members of staff must follow all applicable data protection legislation and school policies when using AILM tools.

- **Ethical Use:** AILMs must be used ethically and in compliance with all applicable laws, regulations, and school policies. Members of staff must not use AILMs to generate content that is discriminatory, offensive or inappropriate.

- **Bias:** AILMs may produce biased, discriminatory or offensive content. Members of staff should use AILMs responsibly and ethically, in compliance with this policy and all other related policies.

- **Security:** All Members of staff must be aware that AILMs may store sensitive data and information, which could be at risk of being breached or hacked.

By using AILMs all members of staff acknowledge that they have read and understood the above and agree to comply with this policy and to report any violations or concerns to the relevant member of staff.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and students 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 about the risks associated with the taking, use, sharing, publication and distribution of images. 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 and carers may take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other students in the digital/video images or take photographs of other students.
- Staff and volunteers can 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR and the Data Protection Act 2018. Please see the school's Data Protection Policy for more details.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table gives details of what is believed to be the appropriate use of these technologies within the school setting.

	Staff		Students		
Use of Technology	**Allowed**	**Not allowed**	**Allowed**	**Only allowed with permission from Assistant Headteacher (Pastoral)**	**Not allowed**
Mobile phones being brought to school	√		√		
Use of mobile phones in lessons		√		√	
Use of mobile phones in social time	√				√
Taking photos on mobile phones or cameras (unless owned by school)		√			√
Use of other mobile devices, e.g. tablets and gaming devices	√*				√
Use of personal email addresses on school network		√			√
Use of school email for personal emails		√			√
Use of social media on school network or school Wifi		√			√

* Must not be used on school Wifi

When using communication technologies:

- Users should be aware that email communications are monitored.
- Users must immediately report 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. Students should report this to their Tutor (who should then report it to the IT team and the Pastoral team) and staff should report it to the IT team.
- Any digital communication between staff and students or parents/carers must be professional in tone and content.
- Students may only use school provided email accounts for educational purposes.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent in an attachment which is password protected.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees during 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 provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, 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, 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.

To put social media in context, it is always worth considering the outcome first. Staff should consider what they are trying to achieve by posting an update or sending a tweet. They can then consider whether social media is the most effective and appropriate method. If social media is simply the most convenient method, then perhaps a slower, but safer and more transparently professional method is required, e.g. email - safer options are out there.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and Illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008				X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986				X
	Pornography			X	
	Promotion of any kind of discrimination			X	
	Threatening behaviour, including promotion of physical violence or mental harm			X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
	Using school systems to run a private business			X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			X	
	Infringing copyright			X	
	Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)			X	
	Creating or propagating computer viruses or other harmful files			X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	
	Online gaming (educational)	X			
	Online gaming (non-educational)			X	
	Online gambling			X	
	Online shopping/commerce			X	
	File sharing		X		
	Use of social media		X*		
	Use of messaging apps		X		
	Use of video broadcasting, e.g. YouTube		X		

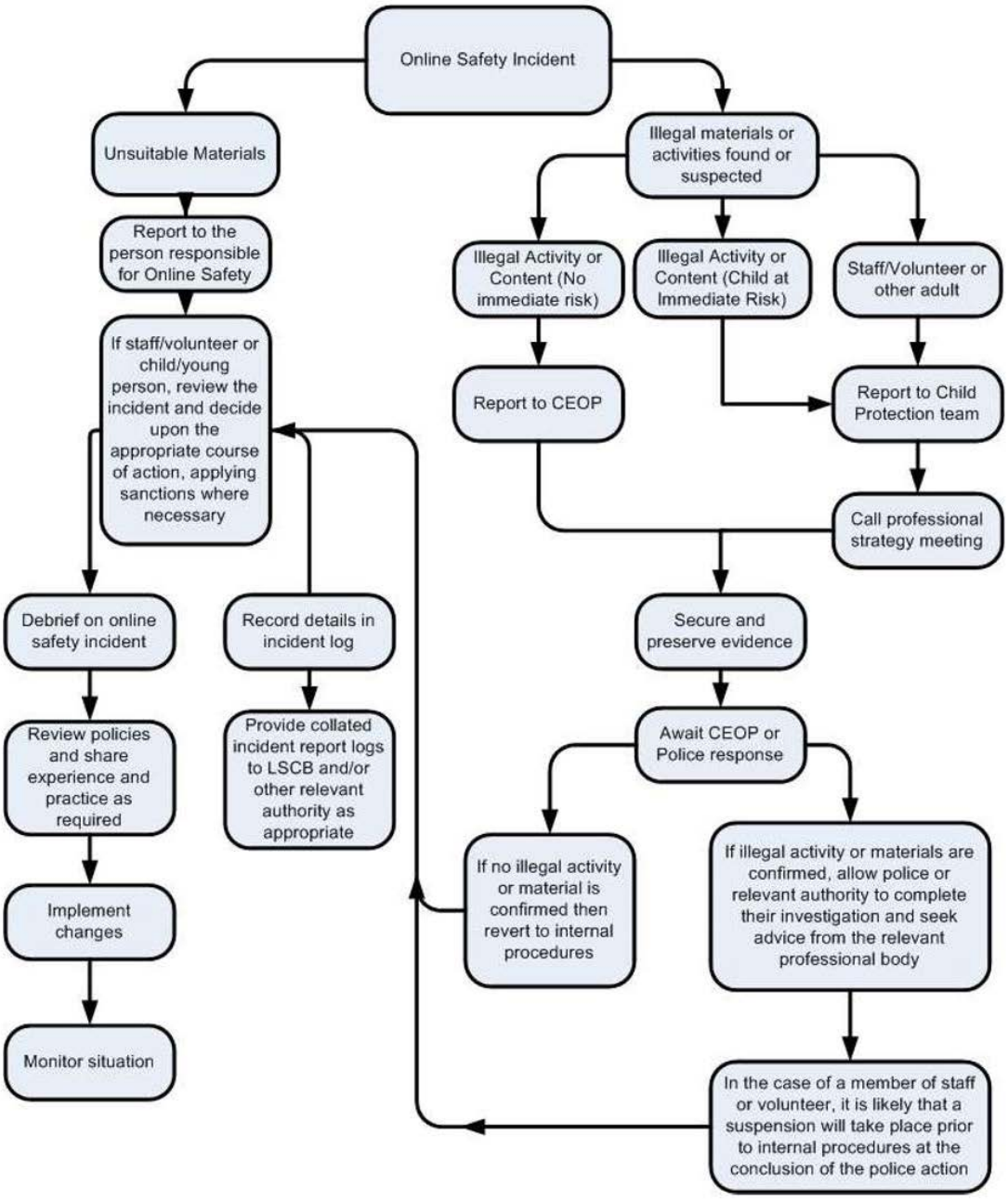
* Risking using personal Social Media accounts for professional reasons could bring disciplinary action. Put simply, using a personal social networking profile for professional contact with a student or parents is a risk – regardless of how professional the motive might be.

Appendix

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services when on the school network or using the school WiFi. It encourages a safe and secure approach to the management of the incident.

Incidents might involve illegal or inappropriate activities (see "User Actions" in the table above). If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart for responding to online safety incidents and report immediately to the police.



Please note that if the school becomes aware of illegal or inappropriate activity by staff or students on their own personal equipment, this is a safeguarding issue and will be investigated by the Designated Safeguarding Lead. The incident will be reported to the police and/or other agencies where appropriate.

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 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 as outlined in the Behaviour for Excellence Policy.