St. John's C. of E.

Blackpool's First Free School 1817

Online Safety Policy

'In everything, do to others what you would have them do to you.'
Matthew 7:12

Be Kind Be Forgiving Be a Good Friend Be Honest Love One Another

Be part of our St John's family!

Last updated: December 2025 Next review date: December 2026

Online Safety Policy

This online safety policy has been developed by Adele Johnston (Online Safety Officer), who has consulted with:

- The Head teacher and Senior Leadership Team
- Staff – including Teachers, Support Staff and volunteers in school
- Technical Support Staff
- Governors
- Parents and Carers
- Pupils in the school
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Aim of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers 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 online-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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the St John's C of E Primary.

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 and updated about online safety incidents and monitoring reports.

The role of the Online safety governor will include:

- regular meetings with the Online safety officers
- Be informed and keep up to date with new filtering and monitoring standards
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Head teacher and Senior Leaders

- The Head teacher 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 officer.
- The Head teacher and governors are responsible for all staff and pupils to adhere to the filtering and monitoring standards at all times.
- The Head teacher and Senior Leadership Team will meet with technical support staff annually to complete a filtering and monitoring audit. Findings from the audit will be shared with governors and all staff.
- The Head teacher and the Designated Safeguarding Leads (DSLs) shall be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head teacher and Senior Leadership Team are responsible for ensuring that the Online safety officer and other relevant staff receive suitable regular and up to date training to enable them to carry out their online safety role and to train other colleagues, as relevant.
- The Head teacher 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 also to support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online safety officer.

Online Safety Officer

- 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 all school staff, parents and governors
- attend regular CPD about online safety, cyber security and the filtering and monitoring standards
- shares regular updates and advice with parents and families about online safety
- liaise with school technical ICT support staff on a weekly basis (Remedian).
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meet regularly with the Online safety governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors if necessary and shares regular updates about the filtering and monitoring standards
- report regularly to the Senior Leadership Team

Technical support staff

In school, the filtering for the internet is provided by Remedian as part of the package that we buy into as a school.

School technical support is also provided by Remedian.

The Online safety officer 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 / other relevant body Online Safety Policy 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher or Senior Leadership Team for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- Liaising with Remedian staff on a weekly basis to ensure that all problems are dealt with efficiently and effectively

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, including the filtering and monitoring standards
- they have read, understood and signed the Staff Acceptable Use Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher or Online safety officer for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems, senior leaders need to be copied in to e-mails between pupils and teachers and also teachers and parents
- online safety issues are embedded in all aspects of the curriculum and other activities and every class is taught about online safety once every half-term (project evolve lessons)
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism, uphold copyright regulations and how to use AI correctly.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. The pupils also need to be taught how to use AI safely and check for accuracy of information.

Designated Safeguarding Leads

Will be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- online-bullying

St John's Pupils

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Use AI safely and only when appropriate.
- 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 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 Policy covers their actions out of school, if related to their membership of the school

St John's Parents

Parents 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, parent workshops, newsletters, letters, school 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
- their children's personal devices in the school
- Appropriate use of social media, demonstrating good practice to their children and ensuring that their children use the websites correctly

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety 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 message 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 lesson from Project Evolve should be provided as part of Computing lessons at least once every half-term and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information, using teaching resources from Project Evolve
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet; particularly around the use of AI
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- All 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. AI should only be used by staff when planning lessons if the information is accurate and suitable.
- 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, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (Remedian) 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 and emailed to the Online safety officer beforehand

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers online safety sessions
- Whole school events e.g. Safer Internet Day
- Reference to the relevant websites

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Education & Training – Staff / Volunteers

It is essential that all school 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 all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- 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.
- The Online safety officer will receive regular updates through attendance at external training events (e.g. from Lancashire / 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 meetings and INSET days.
- The Online safety officer will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions.

This may be offered in a number of ways:

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

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 academy technical systems

- The Head teacher, Senior Leadership Team and technical support (Remedian) will audit the whole school's filtering and monitoring systems annually.
- 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 Online safety officer. Users are responsible for the security of their username and password**.**
- All users will be asked to change their secure password on a regular basis.
- The administrator of passwords for the school ICT system, used by the Online safety officer must also be available to SLT and kept in a secure place.
- The Online safety officer 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. The school filtering system has been checked by the technical staff, Head teacher and Senior Leaders.
    - School technical staff (Remedian staff) continuously monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
    - An appropriate system is in place (please see appendix) for users to report any actual / potential technical incident / security breach to the relevant person – Miss Adele Johnston, or another member of SLT in her absence.
    - 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.
    - An agreed policy is in place (see acceptable user policy for staff and volunteers) regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
    - An agreed policy is in place (see acceptable user policy for staff and volunteers) 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 (e.g. memory sticks / CDs / DVDs) by users on school devices. Staff are instructed to use google drive to store data. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.**

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include; smartphone, tablet, chrome book / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet, which may include the school's learning platform and other cloud-based services such as email and data storage (Google Drive)

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Acceptable Use Agreements for staff, pupils/students 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*	*No*	*Yes*	*No*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*

School owned / provided devices:

- All teaching staff will be provided with a school laptop
- All support staff will be provided with a chrome book
- These devices can be used on or off site
- They can be used for personal tasks as well as work
- Staff may install personal software/apps on their devices so long as it is legal to do so and the device has anti-virus software installed and kept up to date
- Devices should be brought back into school and registered with A Johnston if any issues occur with the device
- Personal data relating to children should not be stored on the device – it should be stored on google drive (secure password protected)
- Staff training on devices will be provided where necessary.
- If a member of staff leaves, they should clear anything personal from devices before returning them to school

Personal devices:

- Staff may use personal mobile devices in school (mobile phones, personal tablets, personal computers) only in areas away from the children
- Pupils are not permitted to use their own devices in school
- Visitors may use personal devices if authorised
- Staff may use personal devices for their own work, but must ensure they have adequate anti-virus software and ensure no data relating to school is stored on their device
- Staff should work on personal devices using google drive and ensure they are signed out of all accounts before switching off their devices
- Staff should ensure that they have pin code protection and the ability to remotely wipe devices if they have school email/calendars on their own devices.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- School has the right to take, examine and search user's devices in the case of misuse
- School does not accept any liability for personal devices that are used for school purposes and become damaged

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils names will not be used on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident, which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy, which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- If they are away from their desk or working area for any period of time they must lock their device.
- Transfer data using encryption and secure password-protected devices.

When personal data is stored on any portable computer system or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. Senior leaders must be copied into e-mail communication between staff and pupils/parents.These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class e-mail addresses may be used in all classes. All of the pupils will be provided with individual school email addresses for educational use.
- 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 and local authorities 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 provides the following measures to ensure reasonable steps are in place to minimize the risk of harm to pupils, staff and the school through limiting access to personal information:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

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 affects 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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities, which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	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	

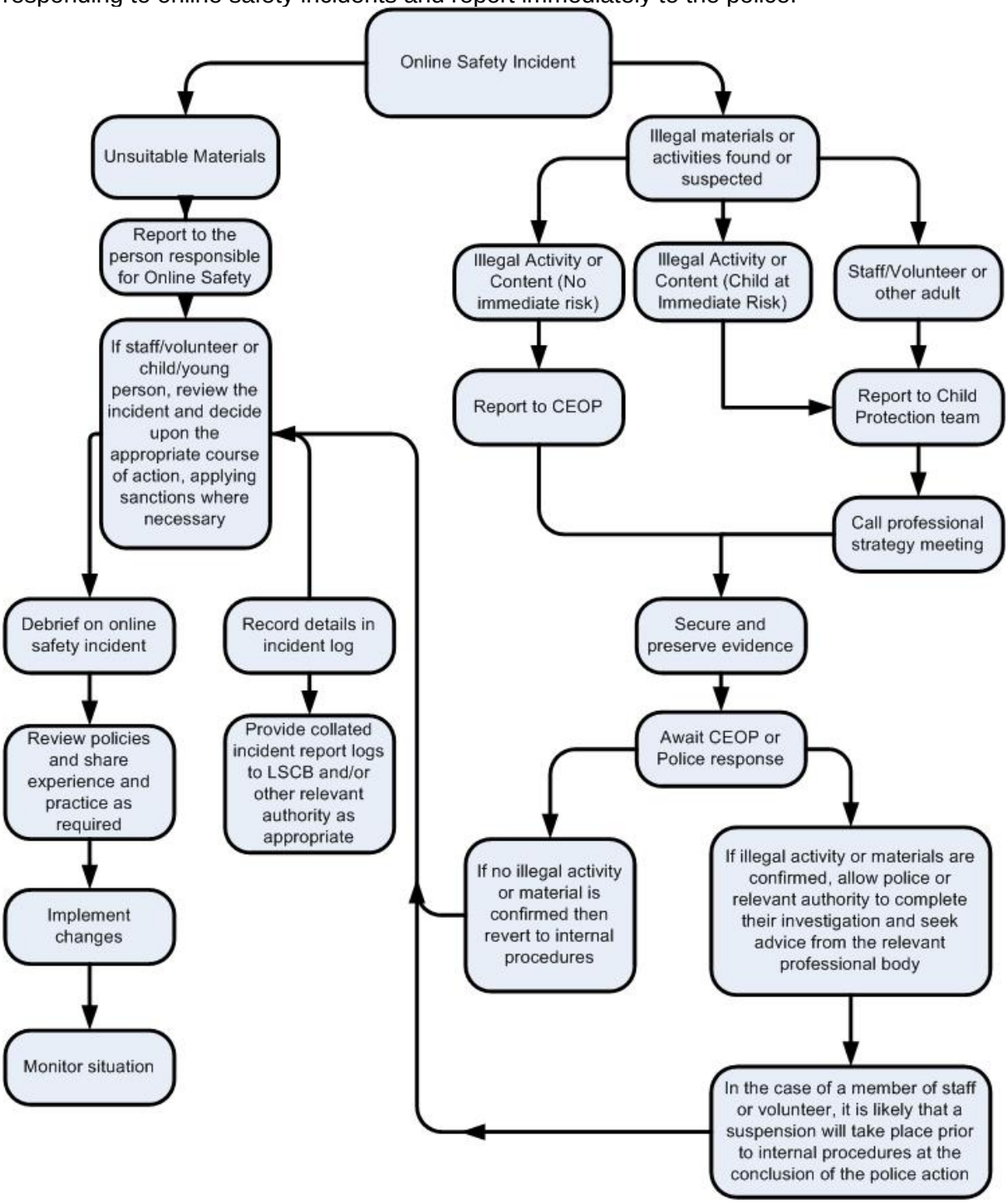
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					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	
On-line gaming (educational)	x					
On-line gaming (non-educational)		x				
On-line gambling		x				
On-line shopping / commerce		x				
File sharing		x				
Use of social media		x				
Use of messaging apps		x				
Use of video broadcasting egYoutube		x				

Responding to incidents of misuse

This guidance is intended for use when staff needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the 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 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 – 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 L A 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 device in question as best you can. Any change to its state may hinder a later police investigation. Do not access or move the device.**

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 follows:

Pupils

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

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher l	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	x				x			
Unauthorised downloading or uploading of files	x				x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x			x			
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x			x	x		
Deliberate actions to breach data protection or network security rules	x	x			x	x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x	x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x			x	x		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x	x			x	x		
Actions which could compromise the staff member's professional standing	x	x			x	x	x	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x		x	x	x	
Using proxy sites or other means to subvert the school's filtering system	x	x	x		x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x			x	x		
Continued infringements of the above, following previous warnings or sanctions	x	x					x	x

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Senior Leaders and ICT technical support (Remedian) to audit the filtering and monitoring standards annually
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff.