St Faith's
Church of England
Infant and Nursery School

Online Safety Policy

"Our inclusive St Faith's family strives to enable all to achieve their full potential and inspire a community of hope and friendship. We seek excellence by ensuring a safe, respectful and flourishing learning community, where differences are celebrated and our genuine love and high expectations make a difference to all."

Oscar Romero …. "Aspire not to have more, but to be more."

PERSON RESPONSIBLE FOR POLICY:	GEMMA WALLIS
APPROVED:	JANUARY 2026
SIGNED:	EMILE VAN DER ZEE
TO BE REVIEWED:	JANUARY 2027

Review of this Policy

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

- Headteacher
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers

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

Schedule for Development/Monitoring/Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	Gemma Wallis – Online Safety Coordinator Amanda Konrath – Safeguarding officers/ Headteacher Ros Garrod-Mason – Governor
Monitoring will take place at regular intervals:	Every Year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Every Year
Should serious online safety incidents take place, the following external persons / agencies should be informed:	InfoTech Direct

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMs
- Monitoring logs of internet activity (including sites visited) / filtering provided by Infotech
    - Kept by Gemma Wallis
- Surveys or questionnaires of Children, parents/carers and staff

Scope of the Policy

This policy applies to all members of the school (including staff, students / Children, volunteers, parents /carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of Children 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.

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

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online Safety Governor, Mrs Ros Garrod-Mason. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governor's meeting

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 Co-ordinator, Mrs Gemma Wallis.

The Head teacher and the members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/other relevant body disciplinary procedures).

The Head teacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The 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 support to those colleagues who take on important monitoring roles.

Online Safety Coordinator

The online safety co-ordinator leads the Online Safety Group and:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff report any online safety incident to the appropriate member of staff.
- 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 online safety governor to discuss current issues, review incident logs and filtering/change control logs.
- Reports, when necessary, to the senior leadership team.

Technical staff – InfoTech Direct

The Technical Staff and Co-ordinator for Computing are responsible for ensuring:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any 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.
- 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, Tapestry, Natterhub, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Online Safety Coordinator for investigation.
- That monitoring software and systems are 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 Staff Acceptable Use Agreement (AUA).
- They follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- They report any suspected misuse or problem to the Headteacher or Online Safety Coordinator for investigation and upload to CPOMs.
- All digital communications with Children should be on a professional level and only carried out using official school devices.
- All digital communications with children, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- They adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- They have a general understanding of how the Children in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- They are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.
- Online safety issues are embedded in all aspects of the curriculum and other activities (see yearly plan and PSHE).
- Children understand and follow the Online Safety Policy and acceptable use agreement.

- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations i.e. searching for royalty free clipart.
- 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 Children 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 Officer

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

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Online Safety Group

The Online Safety Group (Infotech Rep, Ros Garrod-Mason, Gemma Wallis and Digital Leaders) provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- The monitoring of the school Online Safety Policy.
- The monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring incident logs.
- Consulting stakeholders – including parents/carers and the Children about the online safety provision.

Children

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- 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 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.

Families

Adults at home play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. St Faith's will take every opportunity to help parents understand these issues through newsletters, letters, website and information about national/local online safety campaigns and literature. Families are invited to a yearly Internet Safety Chat in school.

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 pupil records.
- Social media accounts – Instagram, Facebook and Natterhub.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks and needs of our children.

We will educate staff and children about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and children will, as always, be at the forefront of our policy and practice.

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and Children for a future in which AI technology will be an integral part. Staff may use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- **We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR**
- **We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities**.
- **We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting children to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping our children with the knowledge, skills and strategies to engage responsibly with AI tools.**
- **As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.**
- **Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.**
- **Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.**

- **We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.**
- **The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the children, being used to train generative AI models without appropriate consent.**
- **AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.**
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating Children to take a responsible approach. The education of Children 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 is provided as part of Computing, PHSE/RSE and other lessons every half term and is regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and activities such as Internet Safety Day.
- Children should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Children should use search terms such as 'royalty free…' when searching for images.
- Children 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.
- **Children should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)**

- **Children should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services**

- Children should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that Children 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 Children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Children are only to access the internet freely after permission given from staff.
- 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 Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Children are to only to use the camera for photographs and videos after seeking permission from a member of staff and of the person to be in the photo.

Education – Families

Parents and carers play an essential role in the education of their children and in the monitoring and 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.

St Faith's will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, school newsletters, web site.
- Digital Leaders newsletters.
- Acceptable use agreement.
- High profile events or campaigns e.g. Safer Internet Day.
- Attending Internet Safety Chats in school.
- Reference to the relevant web sites/publications e.g. 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. 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Coordinator will receive regular updates through attendance at external training events 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
- The Online Safety Coordinator will provide guidance and training to individuals, as required.

Training – Safeguarding Governors

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

- Attendance at training provided by the Local Authority.
- Participation in school/information sessions for staff or parents.

Technical – infrastructure & equipment, filtering & monitoring supported by InfoTech Direct

St Faith's are 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. St Faith's will ensure that Infotech support will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of school technical systems.
- The server in located in the staffroom which is inaccessible to Children, wireless systems and cabling is securely located and physical access restricted from children's access.
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered and regularly updated according to new sites and ratings. 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.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Guest users have access to a 'guest' wireless only to keep the main network protected.
- The school has provided differentiated user-level filtering.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person. (CPOMs)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the extent of personal use that users (staff Children/community users) and their family members are allowed on school devices that may be used out of school.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's iCloud account and email.

All users should understand that the primary purpose of the use mobile or personal devices in a school context is **educational**. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

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

School owned/provided devices:

- All teaching staff have been provided with a laptop for use in the classroom and at home for educational purposes only.
- All staff have access to an iPad for educational purposes such as accessing email, iCloud services and CPOMs.
- All staff laptops and iPads have full network access.
- Technical support provided by Infotech.
- All devices are covered by the acceptable use agreements, filtering and monitoring.
- If staff leave the school, then their devices will be returned and their accounts removed.
- Staff are provided with laptop bags and iPad covers, if these are not used then staff will be liable for damages.

Personal devices:

- The school takes no responsibility for any damage or loss of data while in school.
- Personal devices will not be used for anything that infringes with the data protection and safeguarding policies.
- No technical support will be available for personal devices.
- The school has right to take, examine and search users devices in the case of misuse.
- **Under no circumstances** will personal devices be used to take photographs or videos of children.
- Personal devices should not be used to communicate with Children/parents via video conferencing.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and Children 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.

St Faith's 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 Children 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.
- Permission from parents or carers will be obtained before photographs of Children are published on the school website, social media or local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 Children in the digital and video images.
- Staff and volunteers are allowed to take digital and 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 and video images that Children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include Children will be selected carefully and will comply with good practice guidance on the use of such images.
- Staff should ensure that they have checked the media list that states the preferences of parents for their children on our website, Twitter and other social media.
- Children' full names will not be used anywhere on the website, Twitter, Facebook, particularly in association with photographs.

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- All shared iCloud accounts will have passwords changed when staff/volunteers leave the school.
- 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.
- When leaving a school device unattended, laptops must be closed to restrict access.
- All staff iPads must use the provided passcode.

Only in exceptional circumstances when personal data is stored on any portable computer system, memory stick or any other removable media:

- Personal data must be encrypted and password protected

Cyber security

The DfE Cyber security standards for schools and colleges explains:

> "Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:
>
> - safeguarding issues due to sensitive personal data being compromised
> - impact on student outcomes
> - a significant data breach
> - significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
> - financial loss
> - reputational damage"

The 'Cyber-security in schools: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents schools experience
- the school's education programmes include cyber awareness for Children
- the school has a business continuity and incident management plan in place

There are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Communications

When using communication technologies St Faith's 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. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- **Any digital communication between staff and parents / carers (email, social media, chat, etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1 and EYFS.
- Children 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 and local authorities have a duty of care to provide a safe learning environment for Children 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.

St Faith's provides the following measures to ensure reasonable steps are in place to minimise risk of harm to Children, staff and the school through:

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

School staff should ensure that:

- No personal reference should be made in social media to Children, parents/carers or school and 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.

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

- 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.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Monitoring of Public Social Media

- As part of active social media engagement, St Faith's will pro-actively monitor the Internet for public postings about the school.
- St Faith's will 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 Mrs Konrath, Mrs Wallis and the Online Safety Group to ensure compliance with the school policies.

Unsuitable & inappropriate activities

St Faiths 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	Acceptable for	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on,	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 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

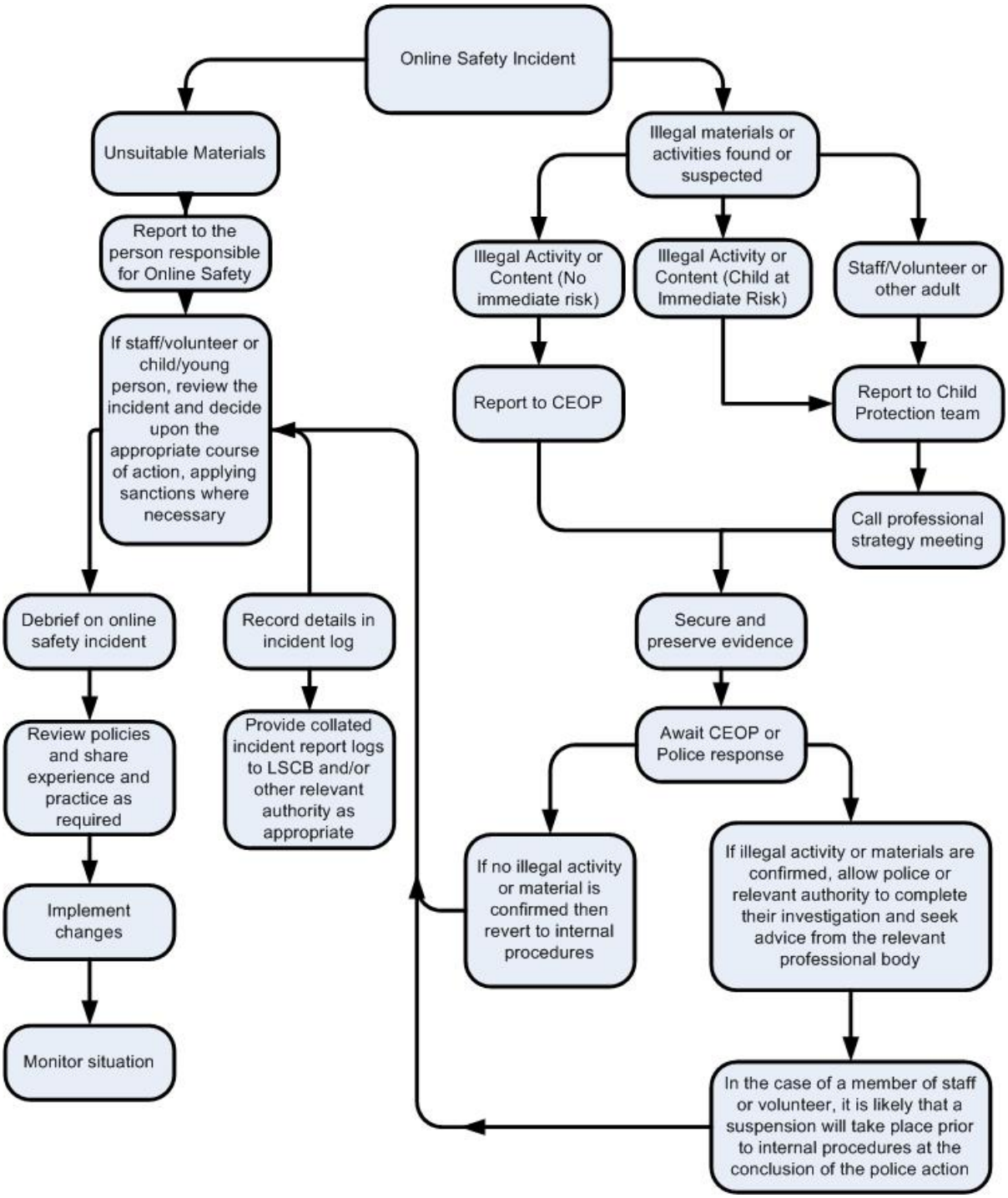
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, apps, 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 (eg 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 e.g. Youtube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need 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 (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 or 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:

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

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

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

The computer in question will be isolated as any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Students / Children Incidents	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X					
Unauthorised use of non-educational sites during lessons	X	X						
Unauthorised of digital camera / iPad	X	X						
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X		X	X			
Corrupting or destroying the data of other users	X							
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	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					

Staff Incidents	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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				
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	x	x				
Actions which breach data protection or network / cyber-security rules.	x	x				
Inappropriate personal use of the internet / social media / personal email	X			X	X	X
Unauthorised downloading or uploading of files				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		
Careless use of personal data e.g. holding or transferring data in an insecure manner				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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / Children	X	X		X	X	X
Actions which could compromise the staff member's professional standing	X			X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X			X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Breaching copyright or licensing regulations	X			X		
Continued infringements of the above, following previous warnings or sanctions	X	X		X		