Children, Young People and Education Directorate

Education Safeguarding Team

Online Safety Policy

St. Saviour's Church of England Junior School

September 2024

Key Details

Designated Safeguarding Lead (s): Nick Bonell – Headteacher

Deputy DSLs: John Arnold – Deputy Headteacher, Suzy Tift – Assistant Headteacher, Sharon Theobald-Grainger - FLO

Safeguarding Governor: Emma Priest

Date agreed and ratified by Governing Body: October 2024

Date of next review: September 2025

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

ST. SAVIOUR'S School Online Safety Policy

1. Policy Aims

- This online safety policy has been written by St. Saviour's involving staff, pupils and parents/carers, building on the The Education People online safety policy template, with specialist advice and input as required. Pupil and parent / carer voice provided through conferencing, school council and parent questionnaire / feedback
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2023,)
- The purpose of St. Saviour's online safety policy is to:
    - Safeguard and protect all members of St. Saviour's community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- St. Saviour's identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. Policy Scope

- St. Saviour's believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- St. Saviour's identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- St. Saviour's believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct

- Behaviour and discipline policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data security
- Image use policy
- Child Protection policy

3. Monitoring and Review

- St. Saviour's will review this policy at least annually
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The school has appointed Nick Bonell as Designated Safeguarding Lead to be the online safety lead.
- St. Saviour's recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a safeguarding culture within the school and its community.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL – Nick Bonell) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure filtering processes shield children from inappropriate content online, whilst allowing children and staff to access relevant learning material.
- Work with our SNS IT support to monitor internet traffic (weekly) in order to identify and deter inappropriate use. NB to log this check on the 'Named Workers / Safeguarding Team Meeting log'
- Ensure that all staff and children understand that our internet feed is filtered and monitored.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly three times per year with the governor with a lead responsibility for safeguarding and/or online safety.
- Meet three times per year with Jez Hoare SNS (ICT support) to assess online safety provision.

4.3 It is the responsibility of all members of staff to:

- Read and sign-off all safeguarding policies on MyConcern.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation lies with the DSL.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Work with the Headteacher to carry out a weekly check of internet use.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- To follow the school procedure if they or others access inappropriate content online.

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home. The school uses Sparkle as a scheme of work for PHSE.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and how to validate information before accepting its accuracy.
    - Teaching pupils to use the internet for research and to verify and compare information.
    - Display online safety posters in classrooms.
    - Teaching pupils how to identify online risks and what to do next.
    - Teach pupils what is acceptable and unacceptable behaviour online.
    - Inform and remind children what to do if they see something inappropriate online in school.
    - Include online safety teaching in Computing lessons.

- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
    - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by pupils.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

5.1.1 Vulnerable Pupils

- St. Saviour's is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- St. Saviour's will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. Online safety will be taught both as discrete topic blocks and in a cross curricular way.
- St. Saviour's will seek input from specialist staff as appropriate, including the SENDCo, Child in Care Lead and IT technical contractors (SNS).

5.2 Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. Refresher training will be delivered as part of ongoing staff meeting and briefing time, as well as small group support staff training
    - This will cover the potential risks posed to pupils (Content, Contact, Commerce and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.
- Reinforce Online Safety across the curriculum, where appropriate, including in assemblies.
- Ensure that children know who they can go to if they need help or have concerns about Online Safety.
- Provide additional Online Safety education for Year 6 to prepare them for transition to secondary school.

5.3 Awareness and engagement with parents and carers

- St. Saviour's recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness events and highlighting online safety at other events such as parent evenings, child-led assemblies to parents (we have found these to have the best uptake,), leaflets by children
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
    - Requiring them to read the school AUP and discuss its implications with their children.

6. Reducing Online Risks

- St. Saviour's recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
    - Regularly review the methods used to identify, assess and minimise online risks.

    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering (RM Safety Net) and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches. All staff are aware that our internet feed is filtered and monitored and they should report anything which may require a change to our filtering or monitoring procedures.

7. Safer Use of Technology

7.1 Classroom Use

- St. Saviour's uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices (IPADS)
    - Internet which may include search engines and educational websites
    - Software such as Scratch,Times table Rockstars, Bookmark, PiXL
    - Email
    - Digital cameras, and video cameras
    - School Instagram and Facebook accounts (specific opt-in consent letters have been issued for school social media image use)
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The school uses RM Safety Net to manage online filtering and children are supervised when using internet equipped devices.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
    - Pupils will use age-appropriate search engines and online tools.
    - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
    - Pupils will only use internet-equipped devices when under the supervision of adults

7.2 Managing Internet Access

- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- St. Saviour's governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over-blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team and SNS contractors will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through RM.
- The school uses RM SafetyNet which blocks sites which can be categorised as: pornography, racial hatred, social networking, extremism, malware, gambling and hacking, gaming and sites of an illegal nature.
- The school works with RM to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off the monitor or put down the mobile device and report the matter to a member of staff immediately
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - SNS IT staff will update and barred lists or filtering settings as needed.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved through RM SafetyNet monitoring tools
- Nick Bonell runs a weekly report of websites used. SNS staff also run a weekly report.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. If a concern is raised from monitoring internet traffic, this is raised with the DSL, Nick Bonell, in line with safeguarding and or staff / pupil conduct guidance.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation. If concerns are identified, the DSL will respond in line with our Child Protection Policy.
- The headteacher has confirmed via SNS that RM is a member of the Internet Watch Foundation

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the GDPR.
    - Full information can be found in the schools Data Protection policy. Our DPO is provided by Invicta Law.

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found AU policies

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.
  - Lock systems when not in use.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online, Video conferencing and webcams

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): Image use policy, GDPR, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.
- If images of children are used on the school website, any permission not granted by our standard consent form, a specific consent form shall be made available for parents / carers to complete.
- Only school devices will be used by the school to make recordings or images of school events, unless express permission is given by the headteacher.

- Staff will use Microsoft Teams and other software to make recordings of teaching for use in the event of the school having to move to online learning. These videos will only be available to pupils via the One Drive.
- All cameras will be disabled or retracted when not in use.
- Staff will be dressed appropriately when videoconferencing / teaching remotely.
- Staff will report any concerns from videoconferencing or online learning to the DSL immediately.

7.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
    - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell Nick Bonell - Headteacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Sensitive safeguarding or personal issues, relating to families or pupils will be sent via MyConcern, this is password protected.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
    - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents. Generally, any email communication from parents or carers will be answered by SLT – this shields staff from spending excessive time answering parental emails. SLT may need to ask staff for information in order to field these queries.
- If staff are contacted via electronic means by pupils or families of pupils, they will immediately inform the headteacher.

7.9 Management of Applications (apps) used to Record Children's Progress

- The school uses Accelerated Reader, Times Tables Rockstars and to track pupils progress and share appropriate information with parents and carers. The school also uses Bookmark, and PiXL.

- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation
- In order to safeguard pupils' data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
    - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.
    - Leaders and staff will monitor the use of learning platforms, including messaging and social media functions. If platforms are used inappropriately, parents / carers will be informed and where content is illegal, the DSL will respond in line with our Child Protection Policy.
    - Members of staff who leave the school shall have access to these platforms removed.
    - All users of online platforms will be advised of their safe / appropriate use.

8. Social Media

8.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of St. Saviour's community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of St. Saviour's community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of St. Saviour's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or which relates directly to St. Saviour's, it's staff or children.
- Social Media sites such as Facebook, TikTok and Instagram are blocked
    - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of St. Saviour's community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as those of the school.
- Members of staff are encouraged not to identify themselves as employees of St. Saviour's on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with the school's policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. St. Saviour's uses I Compute to plan this learning.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications and report concerns both within school and externally.

9. Use of Personal Devices and Mobile Phones

- St. Saviour's recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of St. Saviour's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of St. Saviour's community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used by staff in areas within the school site where children are present.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of St. Saviour's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson. Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless permission has been given by the headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

- If a pupil needs to contact his/her parents or carers they will be allowed to use a telephone in the school office.
- Children must hand over mobile telephones to the school office at the start of the school day. Mobiles should be switched off before hand over and should be collected at 3.20pm

  - Parents are advised to contact their child via the school office during school hours

- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place (the school main office).
  - School staff may confiscate a pupil's mobile phone or device if it has not been handed in to the main office at the start of the day.
  - Searches of mobile phone or personal devices will only be carried out in accordance with www.gov.uk/government/publications/searching-screening-and-confiscation
  - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent / carer. Content may be requested to be deleted, if it contravenes school policies.
  - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day
  - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image Use.
- The school will ensure appropriate information is provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
  - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL will record these issues in line with the school's child protection policy – on MyConcern.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.
- All concerns relating to online safety will be reported on MyConcern.
- Staff will be aware that children present a risk of bullying and abuse to each other (KCSIE Child on Child Abuse). Where such concerns are identified, we will respond in line with our Child Protection Policy. Sanction, support and parental involvement will be used to address any concerns. The school may also involve external agencies or advisors eg. LADO, police or request for support to Front Door Team

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.
- Staff may be offered welfare / support via in-school support (counselling) or via Staff Care Services.

10.3 Parent / Carer Misuse

- Concerns relating to inappropriate conduct or communication online by parents / carers or family members of pupils will be reported as a safeguarding concern and reported via My Concern.
- Concerns may be addressed through writing to the family concerned or by involving KCC Legal, Police or the Front Door Team. Support or advice may be offered in such cases.

11. Procedures for Responding to Specific Online Incidents or Concerns

Our Headteacher, DSL and Deputy DSLs have all accessed and understood Part 5 of Keeping Children Safe in Education 2023. Details of our response to child on child abuse, including sexual violence and abuse can be found in the school Child Protection Policy. St. Saviour's recognises that such abuse can take place online.

Examples of such abuse include:

- Non-consensual or inappropriate sharing of sexual images / videos
- Sexualised online bullying
- Online coercion or threats
- Upskirting or any taking of pictures under a person's clothing – which is a criminal offence
- Unwanted sexual comments or messages online and on social media
- Online sexual exploitation

St. Saviour's will respond to such concerns whether they have occurred in or out of school. When we become aware of such actions we will:

- Notify the DSL and act in accordance with our Child Protection Policy
- If content is on pupils devices, we will act in accordance with the 2022 DfE' Searching, Screening and Confiscation' advice
- Provide safeguards to those concerned, institute safety plans, advice on blocking, reporting and removing online content (to children and families) providing appropriate advice / counselling / pastoral support
- Implement sanctions in line with our Behaviour Policy
- Inform parents / carers of the behaviour / risk and the school's response
- When appropriate, refer such concerns to external agencies such as the police or social services
- If the concern involves pupils at another setting, the DSL will work in partnership with the school's DSL and coordinate a response.
- If a criminal offence has been committed, the DSL or a Deputy DSL will liaise with the police before acting, in order to avoid compromising any subsequent investigation.
- St. Saviour's recognises that victims and perpetrator can be victimised, marginalised / excluded by on and offline communities
- St. Saviour's recognises the potential for repeat victimisation in the future if abuse content continues to exist somewhere online.
- St. Saviour's will ensure that members of the school community are made aware of the potential consequences of online abuse and sexual abuse, violence or harassment.
- We will make all members of the school community aware of sources of information and advice relating to online abuse, sexual abuse and harassment, including child on child abuse.
- Record all incidents and actions on MyConcern.

11.1 Youth Produced Sexual Imagery or "Sexting"

- St. Saviour's recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- St. Saviour's will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with Youth Produced Sexual Imagery

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant KSCMP procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
        - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in DfE guidance.
        - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth-produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

- St. Saviour's will ensure that all members of the community are aware of online child sexual abuse, including: criminal exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- St. Saviour's recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will make members of its community aware of the approaches which may be employed by offenders to target children and understand how to respond.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community, the button is available on the school website.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of an incident involving online sexual abuse of a child, the school will:
    - Act in accordance with the school's Child protection and Safeguarding policies and the relevant KSCMP procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services (if required/ appropriate).
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
    - Record all actions in My Concern.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
    - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- St. Saviour's will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.

- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
    - Act in accordance with the school's child protection policy and the relevant Kent procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
    - Ensure that the headteacher is informed.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St. Saviour's. Concerns will be responded to in line with our CP and Behaviours Policies.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St. Saviour's and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.
- Where appropriate a referral will made to the Prevent Strategy.

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school, through supervision and our monitoring of internet traffic / sites accessed.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

Key Local Contacts

St. Saviour's Designated Safeguarding Lead – Nick Bonell (HT)

Deputy DSLs – John Arnold (DHT), Suzy Tift (AHT) and Sharon Theobald-Grainger (FLO)

Thanet Area Education Safeguarding – 03000 423 157 Online Safety 03000 423 164

LADO 03000 410 888

Police 101 or 999 if immediate risk of harm

Front Door Team 03000 411 111

12. Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
  - esafetyofficer@kent.gov.uk Tel: 03000 423 157
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - Kent e–Safety Blog: www.kentesafety.wordpress.com

KSCMP:

Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk)

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk