St PAUL'S (C OF E) PRIMARY SCHOOL

Online Safety Policy

FAITH – HOPE - LOVE

Reviewed **September 2022**

Next Review **September 2023**

Online Safety Policy

Vision

'We arise, shine and become what God wants us to be'

NIV. "Arise, shine, for your light has come, and the glory of the LORD rises upon you. See, darkness covers the earth and thick darkness is over the peoples, but the LORD rises upon you and his glory appears over you. Nations will come to your light, and kings to the brightness of your dawn. (Isiah 60)

Values
Our values are informed by the values central to Christianity.
They are: Faith, Hope and Love

1. Policy Aims

- This online safety policy has been written by St Paul's C of E Primary School, building on the CEOP recommended online safety policy template.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage and 'Working Together to Safeguard Children' as well as legislation, policy and guidance that seeks to protect children in England from
- The purpose of St Paul's C of E Primary School online safety policy is to:
    - Safeguard and protect all members of St Paul's Primary School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work and to be able 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 Paul's C of E Primary School 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.

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

- We believe that learners should be empowered to build digital resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals are accessing the school network remotely.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Anti-bullying Policy
- SDBE MAT Code of Conduct Policy – included in the Staff Handbook.
- Behaviour Policy
- Safeguarding Policy
- Teaching, Learning and Assessment Policy
- Data Protection Policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. We 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 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 DLS for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Tracey Crannitch, has lead responsibility for online safety.
- St Paul's C of E Primary School 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:

- 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 Staff Code of Conduct Policy, Internet Use Agreement Form – Staff Governors and Volunteers, which covers acceptable use of technology in school – Appendix 1.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and deputy DSLs by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support. These can also be found on the online safety section of the school website.

4.2 The Designated Safeguarding Lead (DSL) 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.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- 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 settings 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 Senior Leadership Team.

- Work with the Senior Leadership Team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the governor with a lead responsibility for safeguarding including online safety.

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting 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 settings 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.
- Liaise with the Network Provider (ICT Educational Services Ltd.) to implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Liaise with the Network Provider (ICT Educational Services Ltd.) to ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Liaise with the Network Provider (ICT Educational Services Ltd.) to ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- 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.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from St Paul's C of E Primary School or the link on the school website, if they or their child encounter risk or concerns online.
- Use our systems, including online subscription sites such as www.mathletics.com , www.spag.com and www.discoveryeducation.co.uk (espresso) and Microsoft Teams, safely and appropriately.
- 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 learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE)/Citizenship, Relationships and Sex Education (RSE) and computing programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- St Paul's C of E Primary School recognises that some learners are 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.

- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the Inclusion Lead.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- St Paul's C of E Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We 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 links to websites on the school newsletter and highlighting online safety at other events such as parent evenings.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- St Paul's C of E Primary School 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 the setting is permitted.
- Ensure that appropriate filtering 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 our computers or devices.

- All members of the community are made aware of our 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 our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- St Paul's C of E Primary School uses a wide range of technology. This includes access to:
  - Laptops and Tablets
  - Internet which may include search engines and educational websites
  - This includes access to: mathletics.com, spag.com, Microsoft Teams and discoveryeducation.co.uk (espresso).
  - Digital cameras, web cams and video cameras via other devices
- All setting owned devices will be used in accordance with our acceptable use policies 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 setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learner's age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learner's age and ability.

7.2 Managing Internet Access

- All staff, learners and visitors will read and sign an Internet Use Agreement Form (Appendix 1) before being given access to our computer system, IT resources or internet.

7.3 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Data Protection Policy.

7.4 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We 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 learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.5 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the photo permission data gathered at entry to St Paul's C of E Primary School (Appendix 3 - Consent Form for taking and using photos).

7.6 Managing Email

- Access to our staff email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider automatically through our email provider.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Tracey Crannitch if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of St Paul's C of E Primary School 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 the school community are expected to engage in social media in a positive, safe and responsible manner.
- All members of the school 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.
- Access to social media in school on personal devices is allowed exclusively in the staffroom.
- Inappropriate or excessive use of social media at school may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of St Paul's C of E Primary School community on social media, should be reported to the DSL 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 our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
- Civil, legal or disciplinary action may be taken if staff 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.
    - 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 that of the setting.
- Members of staff are encouraged not to identify themselves as employees of St Paul's C of E Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and 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 our 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 learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their 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 DSL (or a deputy DSL).
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted.
- Any inappropriate communication from learners and parents received on personal social media accounts will be reported to the DSL (or a deputy DSL).

8.3 Learners Personal Use of Social Media

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- However, we are aware that many of our Key Stage 2 children have social media accounts and, as such, the following will apply:
    - Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
    - Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- In cases where staff are made aware of the social media accounts of Key Stage 2 children, staff may consider the following bullet points:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- 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.
- How to report concerns both within the setting and externally.

9. Use of Personal Devices and Mobile Phones

- St Paul's C of E Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations for Staff

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All members of the school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of the school 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 outside the staffroom and office areas of the school.
- The sending of abusive or inappropriate messages or 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 the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our 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 policy and procedures, such as: child protection, data security and the use of mobile phones in school form – appendix 2
- Staff will be required to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Not use personal devices during teaching periods, unless written 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 learners or parents and carers.
        - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or a deputy DSL).
    - Staff will not use personal devices (unless agreed with a member of SLT and content needs to be deleted once downloaded):
        - To take photos or videos of learners and will only use work-provided equipment for this purpose.
        - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff 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 Learners Use of Personal Devices and Mobile Phones

- Children will hand any mobile devices that they bring into school at the gate. They can collect them at home time at the gate.
- Pupils' mobile devices may not be used at any time on school premises.
- If pupils use their mobile device in school, it will be confiscated and any photographs or other content created during school time will be deleted.

9.4 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- Setting mobile phones and devices must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the ICT Security Acceptable Use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the 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 procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy DSL) will seek advice from the Southwark Safeguarding Children Board.
- Where there is suspicion that illegal activity has taken place, we will contact the Southwark Safeguarding Children Board or Met Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with the Met Police or the Southwark Safeguarding Children Board first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

- The DSL (or a deputy DSL) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputy DSL) will record these issues in line with our Safeguarding Policy using CPOMS.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Southwark Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.
- We will reassure victims that they are being taken seriously and that they will be supported and kept safe. They will not be given the impression they are creating a problem or made to feel ashamed for making a report.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with 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 our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children and child on child abuse

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.
- St Paul's C of E Primary School recognises that sexual violence and sexual harassment between children can take place online and may happen outside of school, online as well as in school. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, online sexual exploitation, content that encourages sexual violence, abusive, harassing, and misogynistic messages, non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups, sharing of abusive images and pornography, to those who don't want to receive such content
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding and Child Protection Policy'.
- We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Well-Being curriculum strand (PSHE/Citizenship and RSE curriculum).
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or a deputy DSL) and act in accordance with our Safeguarding Policy and Anti-Bullying Policy.

- If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our Behaviour Policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Southwark Safeguarding Children Board and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or a deputy DSL) will discuss this with the Met Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

- St Paul's C of E Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or a deputy DSL).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- We 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.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We 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.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) 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 a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with Southwark Safeguarding Children Board.
- Ensure the DSL (or a deputy DSL) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners 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 Southwark Safeguarding Children Board (MASH) and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL 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.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- St Paul's C of E Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or a deputy DSL).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. This is available to access direct from the online safety page on the school website.

- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Safeguarding Policy and the relevant Southwark Safeguarding Children Board procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to MASH (if required/appropriate) and immediately inform Met police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners 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 we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Surrey Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Southwark Safeguarding Children Board by the DSL (or a deputy DSL).

11.4 Indecent Images of Children (IIOC)

- St Paul's C of E Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or a deputy DSL) will obtain advice immediately through the Met police and the Southwark Safeguarding Children Board.
- If made aware of IIOC, we will:
    - Act in accordance with our Safeguarding and Child Protection Policy and the relevant Southwark Safeguarding Children Board procedures.

- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), and the Met police.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or a deputy DSL) 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 setting provided devices, we will:
  - Ensure that the DSL (or a deputy DSL) 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 Southwark Safeguarding Children Board (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 setting provided devices, we will:
  - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying including child on child abuse online

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St Paul's C of E Primary School.
- Full details of how we will respond to any bullying including cyberbullying are set out in our Anti-Bullying Policy and the Children's Anti-Bullying Policy. Copies are available on the school website, and a paper copy from the School Office.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St Paul's C of E Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or a deputy DSL) will obtain advice through the Southwark Safeguarding Children Board and/or the Met Police.

11.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. St Paul's C of E Primary School's contract with ICT Educational Services Ltd includes a web filtering based on a comprehensive education-specific database. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or a deputy DSL) will be informed immediately, and action will be taken in line with our Safeguarding Policy.
- If we are 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 Safeguarding and Child Protection and allegations policies.

Appendix 1

St Paul's (C of E) Primary School

Internet Use Agreement Form -Staff, Governors and Volunteers

St Paul's C of E Primary School will try to ensure that staff, governors and other volunteers have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will expect staff, governors and other volunteers to agree to be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.

St Paul's C of E Primary School aims to ensure that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk and that staff are protected from potential risk in their use of technology in their everyday work

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the system and other users. I recognise the value of the use of digital technology for enhanced learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will educate pupils in my care in the safe use of digital technology and embed online safety in my work with our children, staff, Governors and volunteers

- I understand that the school will monitor my use of the school digital technology and communications systems
- I will not disable or cause any damage to school equipment
- I will immediately report to the premises manager any damage or faults involving equipment or software, however this may have happened.
- I understand that the rules set out in the agreement also apply to use of these technologies out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use
- I will not disclose my user names or passwords to anyone else. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will not engage in any on-line activity that may compromise my professional responsibilities
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted or I have any concerns about the validity of the email
- I will ensure that I will only use my school email address for all electronic communications with pupils, staff, parents, Governors or other volunteers and that all communications are compatible with my professional role
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions

- I will not give out my personal details such as mobile phone numbers and personal email address to pupils or parents
- I will only use the school's digital technology resources and systems for professional purposes.
- I will only use the approved, secure e-mail system for any school business.
- I will not browse, download or send materials that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate person.
- I will not allow unauthorised individuals to access email / internet / intranet / network of other school systems.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- I understand that all internet usage can be logged.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, a laptop or other device to the network that does not have up-to-date anti-virus software.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with the school's Online Safety and Internet Use Agreement Form and Safeguarding Policy
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school website in accordance with school policy.
- I will ensure that any private social networking sites that I create or contribute to or belong to have appropriate levels of security and are not confused with my professional role.
- I will not conduct any communication with a current or ex-pupil via a social network site, such as Facebook, Twitter, Instagram, and Snapchat. Where an ex-pupil is a relative permission should be sought from the Headteacher.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.
- I understand that the school's Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system will be kept private and confidential.
- I will ensure that I am aware of digital safeguarding issues and will embed them within my classroom practice.
- I understand that failure to comply with the Internet Use Agreement Form could lead to disciplinary action.

I agree to abide by the school's Online Safety and Acceptable Use Policy.

Signature …… Date ……..

Full Name ……..

Job Title……

Appendix 2

St Paul's (C of E) Primary School

Use of mobile phones in school

Staff should never contact children, young people or their families from their personal mobile phone, or give their mobile phone number to pupils. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
Mobile phones will not be used during teaching periods in classroom environments or around the school where pupils may be working unless permission has been granted by a member of the senior leadership team in emergency circumstances.
Staff should only make use of mobile phones in designated areas. The designated area is the staff room or staff office. If a private call needs to be made then a request for a room can be made to the Senior Leadership Team or the school office.
Staff should not use personal devices such as mobile phones or cameras at any time to take photos or videos of pupils.
Staff should not send and receive texts in lessons.
Staff will be issued with a school phone where contact with pupils, parents of carers is required, for example, a mobile on school trips or staff based landline in school offices. Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used.
Staff should ensure that their phones and the school mobile are protected with PIN codes in case of loss or theft.
If a member of staff breaches the school policy then disciplinary action will be considered.

I agree to abide by the school's Policy on use of mobile phones in school.

Signature …… Date ……..

Full Name ……..

Job Title……

Appendix 3

St Paul's (C of E) Primary School

Consent form for taking and using photos

Child's name:

Date:

Dear Parents/Carers

At St Paul's C of E Primary School, we take photographs and film pupils as part of our core activity of education. During your child's time at St Paul's C of E Primary School this occurs as part of normal teaching, learning, assessment and safeguarding procedures and as such we do not need your permission for these activities.

However, we do seek your permission to take photographs of your child and use them in the ways described below.

We really value using photos of your child to showcase what they do in school and demonstrate what school life is like to other stakeholders and the wider community.

Furthermore, it is hugely beneficial to be able to identify children with educational, dietary or medical needs to all staff, to safeguard and ensure their well-being.

Please tick all the relevant boxes, sign each item below and return this form to the school office.

I give consent for my child's photo to be stored in SIMS (School Information Management System) as part of their individual data file.

YES ☐ NO ☐ Signed…….

I give consent for my child's photograph to be taken by the school photographer, J P Photographic Limited for individual, group, class and whole school photographs.

YES ☐ NO ☐ Signed…….

I give my consent for photos and videos of my child to be used on the school website (name will be omitted).

YES ☐ NO ☐ Signed…….

I give my consent for photos of my child with their name to be used in classroom, corridor and entrance displays.

YES ☐ NO ☐ Signed…….

I give my consent for photos and the name of my child to appear in local newspapers and magazines. Please note that some newspapers may require the child's full name and may store photographs for online use.

YES ☐ NO ☐ Signed…….

I give my consent for my child to be photographed and filmed by staff and fellow parents during school productions and events as long as it is made clear each time that these must only be used for personal viewing purposes and must not be published in any format including on-line.

YES ☐ NO ☐ Signed…….

I give my consent for my child's image to be used for identification purposes should they have a specific educational, dietary or medical need which needs to be communicated to all staff for safeguarding purposes. (These photographs will be displayed in the staff room and school kitchen only).

YES ☐ NO ☐ Signed…….

Please note: this form is valid for the period of time your child is on roll at St Paul's C of E Primary School. Where the consent is given for a specific reason e.g. a trip, medical condition etc. once this need ends the image will be destroyed by shredding.
If you wish to make any changes, please email the school office at office@stpauls.southwark.sch.uk or call the school on 02077034896 and we will supply you with a new form. If you have any questions, please contact the school office.

Ali Silke
Headteacher

Parent or carer's signature:_____

Date: _____