St James' CE Primary School

Online Safety Policy (including Social Media and Mobile and Smart Technology)

Key Details

Designated Safeguarding Lead (s): (Lucy Hayward, Deputy Headteacher)

Named governor with lead responsibility: (Nina Skomorowski-Brown)

Date written/updated: (Written September 2022, updated January 2023)

Date agreed and ratified by governing body: (21st September 2022)

Date of next review: (September 2023)

This policy will be reviewed **at least** annually. It will also be revised following any changes to technology use, online safety concerns and/or updates to national and local guidance or procedures.

St James' CE Primary School Online Safety Policy

1. Policy Aims and Scope

- This policy has been written by St James' CE Primary School, involving staff, Pupils and parents/carers, building on The Education People policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage 'Working Together to Safeguard Children' and the local Safeguarding Children Multi-agency Partnership procedures, https://www.kscmp.org.uk/ .

- It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. St James' CE Primary School will adopt a whole school approach to online safety which will empower, protect, and educate our pupils and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate

- St James' CE Primary School will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.

- St James' CE Primary School identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - Content: being exposed to illegal, inappropriate or harmful content. For example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - Contact: being subjected to harmful online interaction with other users. For example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
    - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- St James' CE Primary School recognises that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment, which considers and reflects the current risks our children face online.

- The headteacher will be informed of any online safety concerns by the DSL, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- St James' CE Primary School recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online.

- This policy applies to Pupils, parents/carers and 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 school (collectively referred to as "staff" in this policy).

- St James' CE Primary School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

1.1 Policies and procedures

- The DSL has overall responsibility for online safety within the school but will liaise with other members of staff, for example IT technicians and curriculum leads as necessary.

- The DSL will respond to online safety concerns in line with our child protection and other associated policies, including, but not limited to, our Anti-bullying policy, Social Media policy and behaviour policies.
    - Internal sanctions and/or support will be implemented as appropriate.
    - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and the Staff Code of conduct
    - Behaviour and discipline policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data protection
    - Data/information security
    - Cameras and image use policy
    - Mobile and smart technology policy
    - Social media policy
    - Searching, screening and confiscation policy.

- St James' CE Primary School uses a wide range of technology. This includes: computers, laptops, iPad tablets and other digital devices, the internet, our learning platform, intranet and email systems.
    - All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- St James' CE Primary School recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with KCSIE 2022 and EYFS 2021 St James' CE Primary School has appropriate mobile and smart technology and image use policies in place, which are shared and understood by all members of the community. These policies can be found on the school website, SharePoint Policies folder and in the staffroom.

2. Responding to Emerging Risks

- St James' CE 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:

- carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our Pupils face.
- regularly review the methods used to identify, assess and minimise online risks.
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

- Technology evolves and changes rapidly. St James' CE Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.
- All members of the community will be made aware of how the school will monitor policy compliance e.g. Acceptable Use Policies, staff training, classroom management etc.
- 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 online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

4 Responding to policy breaches

4.1 All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures e.g. our child protection and behaviour policies. This includes: breeches of filtering, child on child abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.

4.2 Where pupils breach this policy:

4.2.1 appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.

4.2.2 concerns will be shared with parents/carers as appropriate.

4.2.3 we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.

- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and pupils to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils' parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from the Education People's Education Safeguarding Service or other agency in accordance with our child protection policy.

5 Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Lucy Hayward, Deputy Headteacher) is recognised as holding overall lead responsibility for online safety, however St James' CE Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

5.1 The leadership and management team will:

- Create a whole school culture that incorporates online safety throughout.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies which address the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement. Ensure that staff, Pupils and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all Pupils to develop an appropriate understanding of online safety.

5.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety as appropriate.
- Ensure referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep Pupils safe online, including the additional risks that Pupils with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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 schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the headteacher 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 (termly) with the governor with a lead responsibility for safeguarding.

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

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with Pupils.
- 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 Pupils in their care.
- Identify online safety concerns and take appropriate action by following our safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting Pupils and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

5.4 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 filtering and monitoring and anti-virus software as directed by the leadership team to ensure that the schools IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL to enable them to take appropriate safeguarding action when required.

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

5.6 It is the responsibility of parents and carers to:

- Read our Acceptable Use of technology 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 and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms (Microsoft 365) and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

6 Education and Engagement Approaches

6.1 Education and engagement with Pupils

- St James' CE Primary School will establish and embed a whole school culture and ensure a comprehensive whole school curriculum response is in place to enable all pupils to use the technology in a safe, considered and respectful way and learn about and manage online risks effectively as part of providing a broad and balanced curriculum.
- We and will raise awareness and promote safe and responsible internet use amongst Pupils by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study. At St James' we use Coram Life Scarf Scheme to deliver PSHE and RSHE. Please see the PSHE and RSHE Policy on the school website for more information.
    - reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
    - implementing appropriate peer education approaches, for example E-Safety Mentors.
    - creating a safe environment in which all Pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any Pupils who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our Pupils.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches.

  - providing online safety education as part of the transition programme across the key stages and when moving between establishments.
  - rewarding positive use of technology. This is achieved through positive praise and golden book certificates if appropriate.
- St James' CE Primary School will support Pupils to understand and follow our Acceptable Use policies in a way which suits their age and ability by:
  - sharing our acceptable use policies with them in accessible and appropriate ways.
  - displaying acceptable use posters in all rooms with internet access.
  - informing Pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking Pupil voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- St James' CE Primary School will ensure Pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
  - ensuring age appropriate education regarding safe and responsible use precedes internet access.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - teaching Pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

6.2 Vulnerable Pupils

- St James' CE Primary School recognises that any Pupil can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some Pupils, for example looked after children and those with special educational needs or disabilities, who may be more susceptible or may have less support in staying safe online.
- St James' CE Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to all Pupils who require additional or targeted support. St James' CE Primary School uses the iCompute scheme which includes differentiated learning that can be adapted by teachers to fit the age and development of the pupils they teach.
- Staff at St James' CE Primary School will seek input from specialist staff as appropriate, including the DSLs (Lucy Hayward, John Tutt, Penny Wardell, Sarah Moriarty, Angie Pierce, Sarah Greenfield), SENCO/Designated Teacher (Penny Wardell), and Deputy SENCO (Marissa Noble), to ensure that the policy and curriculum is appropriate to our community's needs.

6.3 Training and engagement with staff

- We will:
  - provide and discuss the online safety policy and procedures, including our acceptable use policy, with all members of staff as part of induction.

- ensure that all staff receive online safety training as part of induction and that ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.
- ensure staff training covers the potential risks posed to Pupils (content, contact and conduct) as well as our professional practice expectations.
- build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
- ensure staff are 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.
- ensure staff are aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with Pupils.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving Pupils, colleagues or other members of the community.

6.4 Awareness and engagement with parents and carers

- St James' CE Primary School recognises that parents and carers have an essential role to play in enabling our Pupils 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, for example highlighting online safety at school events such as parent evenings.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
  - requiring them to read our acceptable use of technology policies and discuss the implications with their children.

- St James' CE Primary School will ensure parents and carers understand what systems are used to filter and monitor their children's online use at school, what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child is going to be interacting with online. This is achieved by:
  - Providing information about our curriculum on our school website and contact notes,
  - Making relevant policies such as acceptable use, home/school agreements available on our school website

- Where the school is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response.

7 Safer Use of Technology

7.1 Classroom use

- St James' CE Primary School uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices
  - Internet, which may include search engines and educational websites
  - Learning platforms, remote learning platform/tools and intranet
  - Email
  - Games consoles and other games-based technologies
  - Programable devices and toys
  - Digital cameras, web cams and video cameras.
- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place. This includes but is not limited to:
  - Filtering and monitoring,
  - Appropriate supervision whilst devices are in use,
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use appropriate search tools as identified following an informed risk assessment. e.g Kidrex, Google Safe Search Kids, BBC Safe Search, SWGfL Squiggle or Doling Kindersley Find Out.
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. This includes: St James' CE Primary School only uses the video sharing platforms Youtube and Microsoft 365 and these are staff access only.
- We 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 internet access and technology use will be appropriate to pupils age and ability. This includes:
  - **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 Pupils age and ability.
  - **Key Stage 2**
    - Pupils will use age-appropriate search engines and online tools.
    - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the Pupils age and ability.

7.2 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, before being given access to our computer system, IT resources or the internet.
- We will maintain a record of users who are granted access to our devices and systems.

7.3 Filtering and monitoring

- St James' CE Primary School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place.
- Our leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- When implementing appropriate filtering and monitoring, St James' CE Primary School will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
-
- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of St James' CE Primary School 's approach to online safety.
- Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment.
- Internet use will be supervised by staff as appropriate to pupils age and ability.
- Pupils will be directed to use age/ability appropriate online resources and tools by staff.

7.3.1 Decision making

- St James' CE Primary School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- St James' CE Primary School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit Pupil's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- 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 will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- Governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- 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 Appropriate filtering

- St James' CE Primary School's education broadband connectivity is provided through Kent County Council and St James' CE Primary School uses KCC and EiS
    - KCC and EiS blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - KCC and EiS is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - KCC and EiS integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

- We work with KCC and EiS to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If pupils or staff discover unsuitable sites or material, they are required to turn off the monitor/screen and report the concern immediately to a member of staff who will report the URL of the site to a DSL and technical staff.
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate in line with existing policies, including child protection, acceptable use and behaviour.
- Parents/carers will be informed of filtering breaches involving pupils.
- Any access to material believed to be illegal will be reported immediately to the relevant agencies, such as the Internet Watch Foundation, the police and/or NCA-Child Exploitation and Online Protection Command (CEOP).

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - physical monitoring (supervision),
    - monitoring internet and web access (reviewing logfile information)
    - and active/pro-active technology monitoring services.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to pupils, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour.
    - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff code of conduct and discipline and conduct policies.

7.4 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 information security policy which can be accessed on SharePoint in the Policies folder or by request made to a member of the Senior Leadership Team.

7.5 Information security and access management

- We take appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and Pupils.
- Further information about technical environment safety and security can be found in our acceptable use policies but includes:
    - 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.
  - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
  - Checking files held on our network, as required and when deemed necessary by leadership staff.
  - The appropriate use of user logins and passwords to access our network and user logins and passwords will be enforced for all users. Individual logins are used for all users including all pupils from Year 1 onwards.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
- St James' CE Primary School will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 1, all Pupils are provided with their own unique username and private passwords to access our systems; Pupils are responsible for keeping their password private.
- We require all users to
  - use strong passwords for access into our system.
  - change their passwords when prompted by the system
  - not share passwords or login information with others or leave passwords/login details where others can find them.
  - not to login as another user at any time.
  - lock access to devices/systems when not in use.

7.6 Managing the safety of our website

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

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct, social media and use of personal devices and mobile phones policies.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct policy.
- 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 to set up personal social media accounts.
- Members of the community will immediately report offensive communication to Lucy Hayward, DSL.
- Excessive social email use can interfere with teaching and learning and will be restricted. It is expected that this will be only accessed out of teaching hours.

7.8.1 Staff email

- All members of staff:
    - are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
    - are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

7.8.2 Pupil email

- Pupils will:
    - use a provided email account for educational purposes.
    - agree an Acceptable Use Policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

- Whole-class or group email addresses will be used for communication outside of the school.

7.9 Educational use of videoconferencing and/or webcams

- St James' CE Primary School recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Videoconferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the Lead DSL or headteacher.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will take place via official and approved communication channels following discussion with a member of SLT, completion of a robust risk assessment and these will be supervised appropriately, according to the pupils age and ability.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the Pupils.

7.10 Management of learning platforms

- St James' CE Primary School uses Microsoft Office 365 as its official learning platform and all access and use takes place in accordance with our acceptable use policies.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, Pupils and parents will have access to the LP. When staff or pupils leave the school, their account will be disabled.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A Pupil's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

7.11 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- St James' CE Primary School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and any local/national guidance.

- All communication with pupils and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and the agreed system, Microsoft 365.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy, staff code of conduct and Acceptable Use Policies.
- Staff and pupils will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. St James' CE Primary School will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

8 Social Media

General social media expectations

- St James' CE Primary School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline and all members of the St James' CE Primary School community are expected to engage in social media in a positive and responsible manner.
- All members of the St James' CE Primary School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school provided devices and systems on site. St James' CE Primary School has appropriate filtering and monitoring systems in place to control access.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary action.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL and/or headteacher prior to use. Any use will take place in accordance with out our remote learning Acceptable Use Policy.
- Concerns regarding the online conduct of any member of St James' CE Primary School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff code of conduct, Acceptable Use Policies, and child protection.

8.1 Staff use of social media

- The use of social media during school hours for personal use is permitted for staff when not in the presence of any pupils.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

8.1.1 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 school. 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. This may include, but is not limited to:

  - Setting appropriate privacy levels on their personal accounts/sites.
  - Being aware of the implications of using location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Using strong passwords.
  - Ensuring staff do not represent their personal views as being that of the school.
- Members of staff are encouraged not to identify themselves as employees of St James'CE Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- 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.

8.1.2 Communicating with pupils and their families

- Staff will not use any personal social media accounts to contact pupils or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media accounts.
- Any communication from pupils and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) or the headteacher.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard pupils, members of staff and the setting.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

8.3 **Official use of social media**

- St James' CE Primary School has no official social media channels however the PTA have a Facebook Page, Parent Rep Facebook Groups, Instagram and Twitter.
- The use of social media sites by St James' CE Primary School PTA only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the headteacher prior to use.
- Official social media sites are suitably protected and, where possible, linked to our website.

    - PTA social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Leadership staff do not have access to account information and login details for the PTA social media channels, however they do check the content periodically.
- PTA social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on PTA social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by the Headteacher or Deputy Headteacher.
- Parents/carers and pupils will be informed of any PTA social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any PTA social media use with pupils; any PTA social media activity involving pupils will be moderated if possible and written parental consent will be obtained as required.
- The PTA will ensure that any PTA social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

8.4 **Pupils use of social media**

- The use of social media during school hours for personal use is not permitted for pupils.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school when the pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection policies and this online safety policy.
- St James' CE Primary School will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies e.g. RSE, PSHE and Computing.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions.
- Pupils will be advised:
    - to consider the benefits and risks of sharing personal details or information 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, for example by making profiles private.
  - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so 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 on social media, both within the setting and externally.
- Any concerns regarding pupils' use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

9 Mobile and Smart Technology

9.1 Safe use of mobile and smart technology expectations

- St James' CE Primary School recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the St James' CE Primary School community are advised to:
  - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of the St James' CE Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our staff code of conduct, behaviour or child protection policies.

9.2 School provided mobile phones and devices

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with pupils or parents/carers is required or to enable site staff to be contactable whilst on site.
- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.
- School mobile phones and devices will be suitably protected via a PIN and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with our staff code of conduct policy, acceptable use of technology policy and other relevant policies.
- Where staff and/or pupils are using school provided mobile phones or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

9.3 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security staff code of conduct and Acceptable Use Policies.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place that is out of sight and reach of pupils during lesson time.
    - Keep personal mobile phones and devices switched off or set 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 written permission has been given by the headteacher or deputy headteacher, such as in emergency circumstances. In the event of a serious behaviour incident, members of staff may use a personal device to contact the headteacher/deputy headteacher if they cannot do so by any other means.
    - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour 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 or circumstance, which could compromise staff’s ability to comply with this, will be discussed with the DSL (or deputy DSL) or headteacher.
- Staff will only use school provided equipment (not personal devices):
    - to take photos or videos of pupils in line with our image use policy.
    - to work directly with pupils during lessons/educational activities.
    - to communicate with parents/carers.

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.4 Pupils use of mobile and smart technology

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies e.g. PSHE, RSE and Computing.
- Mobile phones and/or personal devices will not be used on site by pupils.
- St James' CE Primary School does not allow pupils to bring personal devices and mobile phones to school except with written permission from the headteacher, given in exceptional circumstances. For those pupils who are given permission, St James' CE Primary School expects pupils' personal devices and mobile phones to be handed in to the class teacher who will store them out of reach of other children, other than when being used for the permitted purpose.
- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone in the office.
    - Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.
- If a pupil requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the pupil and their parents carers before use is permitted.
- Where pupils' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

9.4.1 Screening, searching and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding pupils' use of mobile technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.

- Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
- Mobile phones and devices that have been confiscated will be held by a member of SLT in a secure place and released to parents/carers at the end of the day or after a longer period for a repeat offence.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files 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

- If deemed to be necessary and appropriate, searches of mobile phones or personal devices may be carried out in accordance with our behaviour policy which can be found on the school website and the DfE 'Searching, Screening and Confiscation' guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy which can be found on the school website.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy, which can be found on the school website, and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

9.5 Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that mobile phones are not used in any area except the office waiting area, unless permission is granted by the headteacher/deputy headteacher for use for a specific purpose, for example, as part of multi-agency working arrangements.
- Appropriate signage and information are in place in the office entrance area to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL (or deputy) or headteacher of any breaches of our policy.

10 Procedures for Responding to Specific Online Concerns

Please see our Child Protection Policy, which can be found on the school website, for more information about each of these specific concerns.

10.1 Online child on child abuse

- St James' CE Primary School recognises that whilst risks can be posed by unknown individuals or adults online, Pupils can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online peer on peer abuse can take many forms, including but not limited to:
    - bullying, including cyberbullying, prejudice-based and discriminatory bullying
    - abuse in intimate personal relationships between peers
    - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
    - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
    - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
    - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
    - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
    - initiation/hazing type violence and rituals.

- St James' CE Primary School believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- St James' CE Primary School believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- St James' CE Primary School recognises that, even if there are no reported cases of online peer on peer abuse, such abuse is still likely to be taking place.
- Concerns about Pupil's behaviour, including peer on peer abuse taking place online offsite will be responded to as part of a partnership approach with Pupils and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies.
- St James' CE Primary School want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online peer on peer abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Pupils who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, St James' CE Primary School will follow the guidance outlined in Part Five of KCSIE 2021 and the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' guidance.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- St James' CE Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- St James' CE Primary School recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and 24 services, and for things to move from platform to platform online.
- St James' CE Primary School 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.
- St James' CE Primary School 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 and the support available, by implementing a range of age and ability appropriate

educational methods as part of our curriculum for example, our computing, RSE and PSHE curricula and policies.

- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children, and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the Police. Advice may be sought via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website.
    - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
    - If content is contained on Pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Following an immediate risk assessment the school will:
    - provide the necessary safeguards and support for all Pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
    - if the concern involves children and young people at a different educational school, the DSL will 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 will discuss this with the 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.
- St James' CE Primary School recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. St James' CE Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing

- St James' CE Primary School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
    - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
    - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
    - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and/or semi-nude imagery, St James' CE Primary School will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- St James' CE Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods e.g. our Computing, RSE and PSHE curricula and policies.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
    - Report any concerns to the DSL immediately.
    - Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
    - Not delete the imagery or ask the child to delete it.
    - Not say or do anything to blame or shame any children involved.
    - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
    - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
    - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
    - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of Pupils involved, including the possibility of carrying out relevant checks with other agencies.
    - a referral will be made to Children's Social Care and/or the police immediately if:
        - the incident involves an adult (over 18).
        - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
        - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
        - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
    - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
    - If DSLs are unsure how to proceed, advice will be sought from the local authority via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website.
    - Store any devices securely:

        - If content is contained on Pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially 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.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
    - provide the necessary safeguards and support for Pupils, such as offering counselling or pastoral support.
    - implement sanctions where necessary and appropriate 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 UKCIS 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.
        - Pupils will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
    - 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.
- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. DSLS will follow 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and, if it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request pupils to do so.

10.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St James' CE Primary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which can be found on our school website.

10.2 Online child abuse and exploitation

- St James' CE Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection policy.
- St James' CE Primary School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers in line with our Computing, RSE and PSHE curricula and policies.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
- store any devices containing evidence securely:
  - If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
- if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a pupil is at immediate risk. Advice may be sought via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website.
- 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 and provide support and signposting, as 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; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
  - Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority (via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website) and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to pupils and other members of our community. This can be accessed at the bottom of any page on our school website.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.
- If members of the public or Pupils at other schools are believed to have been targeted, the DSL, will seek advice from the police and/or the Local Authority (via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website) before sharing specific information to ensure that potential investigations are not compromised.

10.3 Indecent Images of Children (IIOC)

- St James' CE Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will 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 will obtain advice immediately through the police and/or the Local Authority (via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website).
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures (via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website).
    - store any devices involved securely, until advice has been sought. If content is contained on Pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a Pupil has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by Pupils.
    - report concerns as appropriate to parents and carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children, we will:
    - ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police in accordance with our managing allegations against staff policy.
    - quarantine any involved school provided devices until police advice has been sought.

10.4 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at St James' CE Primary School and will be responded to in line with existing policies, including child protection, 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 will obtain advice through the Local Authority (via the Kent Education Safeguarding Service. Contact details can also be found in our Child Protection Policy which can be found on the school website) and/or the police.

10.5 Online radicalisation and extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. Please see Section 6.2 of this policy for more information about Filtering and Monitoring.
- If we are concerned that a pupil or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy:
    - If the concerns relate to a member of staff, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

10.6 Cybercrime

- St James' CE Primary School recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

11 Useful Links

Additional links can be found in annex D of Keeping Children Safe In Education 2022.

Kent Safeguarding Service Online Safety

- 03301 651 500

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 360 Safe Self-Review tool for schools www.360safe.org.uk
- Childnet: www.childnet.com
    - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
  - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk