



The Saints Academies Online Safety Policy

Reviewed and revised September 2026

Next review September 2027

1. Policy Aims

This policy takes into account the DfE statutory guidance [Keeping Children Safe in Education 2026](#). In line with this guidance, The Saints Academies recognises that online safety is an essential part of safeguarding and that children may be exposed to a range of risks through their use of technology.

The Saints Academies recognises the online risks associated with misinformation and disinformation, as well as risks arising from new and emerging technologies, including artificial intelligence (AI) and generative AI tools. These risks will be addressed through age and developmentally appropriate education, staff training, effective supervision, appropriate filtering and monitoring, and safeguarding procedures.

The purpose of this online safety policy is to:

- Safeguard and protect all members of The Saints Academies when using technology and accessing online services.
- Identify approaches to educate learners about online safety in ways that are appropriate to their age, developmental stage and individual needs.
- Raise awareness of online safety throughout the school community, including with staff, parents and carers.
- Enable all staff to work safely and responsibly, model positive and professional behaviour online and maintain appropriate professional standards when using technology.
- Ensure that new and emerging technologies, including AI and generative AI tools, are used safely, appropriately and responsibly within the academies.
- Identify clear procedures for recognising, reporting and responding to online safety concerns.
- Provide staff with regular and up-to-date online safety information, guidance and training.



The Saints Academies recognises that online safety issues are wide-ranging but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, including misinformation and disinformation.
- **Contact:** being subjected to harmful online interaction with other users.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** risks such as inappropriate advertising, phishing, scams and other financial harms.

These risks will be considered in an age and developmentally appropriate way, recognising the needs and experiences of the children within our academies.

2. Policy Scope

- The Saints Academies recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children and staff are protected from potential harm online.
- The Saints Academies recognises that the internet and associated technologies and devices, including computers, tablets, mobile phones, games consoles, smart and connected devices, and AI-enabled technologies, are an important part of everyday life.
- The Saints Academies believes that children should be supported to develop the knowledge, skills and resilience needed to use technology safely and responsibly, in ways that are appropriate to their age, developmental stage and individual needs.
- This policy applies to all staff, including the LAC, 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 children, parents and carers.
- This policy applies to any access to the internet and use of technology, including personal devices, and where staff or other individuals have been provided with setting-issued devices for use off-site, such as work laptops, tablets or mobile phones.

2.1 Links with other policies and practices

This policy should be read alongside relevant academy policies and statutory guidance, including:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policies



- Computing Policy
- PSHE and Relationships Education/RSE policies
- Data Protection Policy and UK GDPR procedures
- Mobile Phone and Personal Devices Policy/procedures
- Images and Photography Policy/procedures
- Managing Allegations Against Staff procedures
- Whistleblowing Policy
- Keeping Children Safe in Education 2026

3. Monitoring and Review

- Technology and online risks evolve and change rapidly. This policy will be reviewed at least annually, or sooner where required by changes to statutory guidance, legislation, technology or identified safeguarding risks.
- Reviews will take account of online safety incidents, filtering and monitoring reports, stakeholder feedback and new or emerging risks, including those associated with artificial intelligence (AI) and generative AI.
- The policy will also be reviewed following significant online safety or child protection concerns, changes to national or local requirements, or significant changes to the academy's technical infrastructure or use of technology.
- The effectiveness of the academy's filtering and monitoring provision will be reviewed at least once every academic year, in line with [Keeping Children Safe in Education 2026](#) and the DfE [Filtering and Monitoring: Core Standard](#).
- The filtering and monitoring review will involve appropriate members of the Senior Leadership Team, the Designated Safeguarding Lead (DSL), IT support and the responsible member of the Local Academy Council (LAC). The outcome of the review and any actions identified will be formally recorded.
- Appropriate checks of filtering and monitoring systems will take place during the academic year. The frequency and nature of these checks will reflect the academy's context, the age and needs of its children and any risks identified through safeguarding and risk assessment processes.



- Filtering and monitoring arrangements will also be considered when introducing new technology, devices, systems or generative AI tools.
- The Executive Headteacher/Deputy Headteacher will be informed of online safety concerns, as appropriate.
- The Local Academy Council will receive appropriate information about online safety practice, filtering and monitoring arrangements, incidents and outcomes to enable effective safeguarding oversight.
- Any issues or areas for improvement identified through monitoring and review will be incorporated into the academy's action planning.

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL), with support from the Computing Coordinator, has lead responsibility for online safety.

The Saints Academies recognises that online safety is an essential part of safeguarding and that all members of staff have important roles and responsibilities in keeping children safe online.

A member of the Senior Leadership Team and a member of the Local Academy Council (LAC) will have identified responsibility for ensuring that the DfE Filtering and Monitoring Standards are met.

4.1 The leadership and management team will:

- Ensure that online safety is recognised as a safeguarding issue and that practice is in line with national and local guidance and requirements.
- Ensure there are appropriate and up-to-date policies relating to online safety, including a Staff Code of Conduct and Acceptable Use Policies covering the safe and appropriate use of technology.
- Ensure suitable and appropriate filtering and monitoring systems are in place and work with the DSL, Computing Coordinator and technical support to monitor the safety and security of systems and networks.
- Ensure that roles and responsibilities for filtering and monitoring are clearly identified and understood.
- Ensure that filtering and monitoring provision is reviewed and checked in accordance with current DfE standards and that the outcomes and any actions are recorded.
- Ensure that online safety is embedded within a progressive curriculum which enables all children to develop an age and developmentally appropriate understanding of online safety.
- Ensure that the risks and opportunities associated with new and emerging technologies, including artificial intelligence (AI) and generative AI, are appropriately considered before their use within the academies.



- Support the DSL and Computing Coordinator by ensuring they have sufficient time, training and resources to fulfil their online safety responsibilities.
- Ensure there are clear and accessible reporting routes for children, staff, parents and carers to raise online safety concerns.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) with support from the Computing Coordinator will:

- Act as a named point of contact for online safeguarding issues and liaise with other members of staff, technical support or external agencies, as appropriate.
- Ensure online safety is recognised as part of the academies' safeguarding responsibilities and that a coordinated approach is implemented.
- Understand the filtering and monitoring systems and processes in place within the academies.
- Work with the leadership team and technical support to ensure that filtering and monitoring arrangements are appropriate to the age, developmental stage and needs of the children.
- Review relevant filtering and monitoring reports and respond promptly to safeguarding concerns identified through monitoring.
- Ensure that appropriate action is taken and recorded where filtering or monitoring identifies a safeguarding concern.
- Provide the LAC with appropriate assurance that filtering and monitoring systems are working effectively and are regularly reviewed.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training, including an understanding of their responsibilities for filtering and monitoring.
- Access appropriate training and support to maintain an up-to-date understanding of online safety risks, including risks associated with emerging technologies and AI.
- Recognise and understand the additional online risks that may be experienced by vulnerable children, including children with Special Educational Needs and Disabilities (SEND).
- Keep up to date with current research, legislation, statutory guidance and emerging online safety risks and communicate relevant information to staff and the wider school community.
- Work with staff to coordinate participation in appropriate local and national events that promote positive and safe online behaviour, such as Safer Internet Day.
- Promote online safety awareness with parents, carers and the wider school community.



- Maintain accurate records of online safety concerns, actions, decisions and outcomes as part of the academies' safeguarding recording procedures.
- Monitor online safety incidents to identify patterns, emerging risks or gaps in provision and use this information to inform curriculum, training, policies and procedures.
- Report online safety concerns and trends, as appropriate, to the leadership team and LAC.
- Work with the leadership team to review and update online safety policies at least annually, or sooner where required.

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

- Read, understand and adhere to the Online Safety Policy and relevant Acceptable Use Policies.
- Take responsibility for the security of academy systems, devices and data they use or have access to.
- Model safe, responsible and professional use of technology, both on and off site.
- Embed age and developmentally appropriate online safety education within curriculum delivery and reinforce safe online behaviours whenever technology is used.
- Maintain an awareness of online safety risks and understand how these may affect children of different ages, abilities and needs.
- Understand their role in relation to filtering and monitoring and remain vigilant when children are using technology; filtering and monitoring systems do not replace effective supervision.
- Report any concerns about inappropriate or harmful online content, filtering or monitoring breaches, or other online safety concerns promptly in accordance with safeguarding procedures.
- Identify online safety concerns and take appropriate action by following the academies' safeguarding policies and procedures.
- Know when and how to escalate online safety concerns and where appropriate support can be accessed.
- Use only academy-approved systems, applications and AI tools for school business.
- Ensure that personal, sensitive or confidential information about children, families, staff or the academy is not entered into unapproved AI or generative AI tools.
- Take responsibility for maintaining their knowledge and professional development in relation to online safety and emerging technologies.

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

- Provide appropriate technical support and advice to the DSL, Computing Coordinator and leadership team in relation to online safety, filtering, monitoring and information security.



- Implement appropriate security measures, as directed by the leadership team, to ensure that academy IT systems and networks are secure and protected from misuse or malicious attack, while enabling appropriate educational use.
- Implement and maintain appropriate filtering and monitoring systems in accordance with the academy's agreed requirements and current DfE standards.
- Ensure filtering and monitoring systems are appropriately configured, maintained and updated.
- Provide appropriate access to filtering and monitoring information and reports to the DSL and leadership team so that safeguarding concerns can be identified and acted upon promptly.
- Promptly escalate technical concerns, system failures, filtering or monitoring issues and potential safeguarding risks to the appropriate member of the leadership team and/or DSL.
- Support the academy in carrying out regular checks and the annual review of filtering and monitoring provision.
- Maintain appropriate records of significant changes made to filtering and monitoring systems.

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

- Take part in age and developmentally appropriate online safety learning.
- Follow the academy's simple rules for safe and responsible use of technology.
- Use academy devices and technology carefully and appropriately.
- Be kind and respectful to others when using technology.
- Ask a trusted adult before accessing unfamiliar websites, apps or online content.
- Tell a trusted adult if they see or experience anything online that makes them feel worried, uncomfortable, confused or unsafe.
- Understand, at an age-appropriate level, that personal information should be kept private and not shared without permission.
- Seek help from a trusted adult when something goes wrong online.

4.6 It is the responsibility of parents and carers to:

- Support the academy's approach to online safety by discussing online safety with their child and reinforcing safe and appropriate use of technology at home.
- Support their child to access online content, games, apps and services that are appropriate for their age and developmental stage.
- Be aware of age restrictions and parental controls relating to the online services, games, apps and devices their child uses.
- Role model safe, respectful and responsible use of technology and social media.



- Encourage their child to talk to a trusted adult if anything online worries, upsets or confuses them.
- Be alert to changes in behaviour that may indicate that their child has experienced harm or inappropriate content online.
- Seek help and support from the academy or appropriate agencies if they or their child encounter an online safety concern.
- Engage with online safety information, guidance and opportunities provided by the academy.
- Support academy expectations regarding acceptable use of technology and personal devices.

5 Education and Engagement Approaches

5.1 Education and engagement with children

The Saints Academies will provide a progressive and age and developmentally appropriate online safety curriculum which enables children to develop the knowledge, understanding and skills they need to use technology safely and responsibly.

We will:

- Ensure that children receive appropriate online safety education before and alongside their use of internet-enabled technology.
- Teach online safety through appropriate areas of the curriculum, including Computing, PSHE and Relationships Education/RSE.
- Reinforce online safety messages whenever children use technology or access online content.
- Teach children, at an age-appropriate level, to understand that not everything they see or hear online is true, accurate or trustworthy.
- Support children to develop appropriate critical thinking skills as they become older and more independent in their use of technology.
- Teach children about personal information and the importance of not sharing information about themselves or others without permission.
- Teach children that people they communicate with online may not always be who they say they are.
- Teach children about respectful and kind behaviour when using technology and communicating with others.
- Teach children to recognise when something they see, hear or experience online makes them feel worried, uncomfortable, confused or unsafe and to tell a trusted adult.
- Teach children how to seek help and report concerns in ways appropriate to their age and ability.



- Introduce children, where appropriate, to the idea that digital content, including images, videos and information, can be created, changed or generated using technology, including artificial intelligence (AI).
- Ensure that any teaching about AI and emerging technologies is appropriate to children's age and developmental stage and focuses on safe, responsible and supervised use.

The Saints Academies will support children to understand and follow Acceptable Use expectations in ways appropriate to their age and ability by:

- Using simple, child-friendly Acceptable Use rules and posters.
- Explaining that use of academy devices and internet access may be monitored to help keep everyone safe.
- Seeking children's views, where appropriate, when developing online safety education and practices.
- Using appropriate resources, visitors and national initiatives, such as Safer Internet Day, to complement the academy's online safety curriculum.

5.2 Vulnerable Learners

The Saints Academies recognises that some children may be more vulnerable to online risks 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), children with additional communication needs, children with English as an Additional Language (EAL), and children experiencing trauma, loss or other vulnerabilities.

We recognise that some children may require additional support to recognise online risks, understand appropriate boundaries, communicate concerns or seek help.

The Saints Academies will ensure that online safety education, supervision and support are adapted to meet children's individual needs, age, ability and developmental stage.

Where appropriate, the DSL will work with relevant staff, including the SENCO, teachers and other professionals, to identify and provide additional online safety support for vulnerable children.

5.3 Training and engagement with staff

The Saints Academies will:



- Provide all members of staff with the Online Safety Policy, relevant procedures and Acceptable Use expectations as part of their induction.
- Provide regular, up-to-date and appropriate online safety training as part of safeguarding training and professional development.
- Ensure staff understand the four areas of online risk: **Content, Contact, Conduct and Commerce**.
- Ensure staff understand their responsibilities in relation to filtering and monitoring and know how to report concerns or breaches.
- Ensure staff receive appropriate information and training about new and emerging online risks, including artificial intelligence (AI), generative AI, manipulated content and deepfakes.
- Ensure staff understand the importance of protecting children's personal and confidential information when using technology, online services and AI tools.
- Ensure staff know that personal, sensitive or confidential information must not be entered into unapproved AI or online systems.
- Recognise the knowledge and expertise staff develop through safeguarding training and managing concerns and provide opportunities for staff to contribute to online safety policies and practice.
- Make staff aware that use of academy IT systems may be monitored and that activity may be attributable to individual users.
- Remind staff that their online conduct, including their personal use of social media, must remain consistent with professional standards and may have an impact on their professional role and reputation.
- Provide staff with appropriate online safety guidance, resources and updates relevant to the ages and needs of the children within the academies.
- Ensure all staff understand the procedures for reporting online safety concerns involving children, colleagues or other members of the academy community.

5.4 Awareness and engagement with parents and carers

The Saints Academies recognises that parents and carers have an essential role in helping children to become safe, responsible and confident users of technology.

We will work in partnership with parents and carers by:

- Providing regular information, guidance and updates about online safety and emerging online risks.
- Providing or signposting parents and carers to guidance about age restrictions, parental controls, privacy settings and the safe use of apps, games, social media, connected devices and emerging technologies.



- Encouraging parents and carers to talk regularly with their children about what they do, watch and experience online.
- Encouraging the use of age-appropriate content, services and games and appropriate adult supervision, particularly for younger children.
- Helping parents and carers understand how to respond if their child encounters inappropriate content, unwanted contact or another online safety concern.
- Promoting online safety events and initiatives, including Safer Internet Day.
- Drawing parents' and carers' attention to the Online Safety Policy and relevant expectations through appropriate academy communications and the academy website.
- Providing online safety information to families when children join the academies.
- Asking parents and carers to support the academy's Acceptable Use expectations and discuss age-appropriate online safety rules with their children.
- Signposting parents and carers to appropriate sources of further support where necessary.

6. Reducing Online Risks

The Saints Academies recognises that the online environment is constantly changing, with new websites, apps, games, devices, services and technologies emerging rapidly.

To reduce online risks, The Saints Academies will:

- Regularly review the approaches used to identify, assess and minimise online risks.
- Consider the age, developmental stage, individual needs and vulnerabilities of children when assessing online risks and deciding whether technology is appropriate for use.
- Assess new websites, apps, online services, devices and emerging technologies, including artificial intelligence (AI) and generative AI tools, before they are introduced for use within the academies.
- Consider the educational benefit, age appropriateness, privacy, data protection and safeguarding implications of new technologies before their use is approved.
- Ensure appropriate filtering and monitoring systems are in place, in accordance with current DfE standards, to reduce children's exposure to harmful and inappropriate online content.
- Ensure that filtering and monitoring systems are supported by effective adult supervision and age and developmentally appropriate online safety education.
- Review filtering and monitoring arrangements when new technology, devices, services or systems are introduced.
- Ensure staff know how to report inappropriate or harmful content and any concerns about the effectiveness of filtering or monitoring systems.



- Respond promptly to identified online safety risks and take appropriate safeguarding, technical or educational action.

The Saints Academies recognises that, due to the changing and connected nature of the internet, it is not possible to guarantee that unsuitable material will never be accessed. Filtering and monitoring systems do not replace effective supervision, education and professional vigilance.

All members of The Saints Academies will be made aware, at a level appropriate to their age and role, of expectations for safe, respectful and responsible online behaviour. Content, comments, images or videos that may cause harm, distress or offence must not be created, accessed or shared using academy systems or devices.

These expectations are reinforced through the academy's Acceptable Use Policies, safeguarding procedures, curriculum and staff training.

7. Safer Use of Technology

7.1 Classroom Use

The Saints Academies uses a range of technology to support teaching and learning. This may include:

- Computers, laptops and tablets, including iPads.
- Internet access, including approved websites, search tools and educational resources.
- Digital cameras, webcams and video-recording equipment, including cameras on academy devices.
- Programmable and computing devices, such as Bee-Bots.
- Interactive teaching technology.
- Other approved digital, connected or AI-enabled technologies.

All academy-owned devices and technology will be used in accordance with our Acceptable Use Policies and with appropriate safety, security, filtering and monitoring measures in place.

Staff will evaluate websites, apps, online tools and digital resources before using them with children or recommending them for use at home. Consideration will be given to their educational purpose, age appropriateness, content, privacy, data protection and safeguarding implications.

Children will only access online content, tools and services that are appropriate to their age, developmental stage and learning needs.



Children will be supported, at an age and developmentally appropriate level, to understand that information, images and videos found online may not always be accurate or trustworthy and that digital content can be created or changed using technology, including artificial intelligence (AI). Adult supervision of children's use of technology and internet access will be appropriate to their age, ability and developmental stage.

Early Years Foundation Stage and Key Stage 1

Access to the internet will primarily be through adult demonstration or directly supervised access to specific, approved online materials and resources which support planned learning. Children will be taught simple, age-appropriate online safety messages and encouraged to seek help from a trusted adult whenever they are unsure, worried or uncomfortable about something they encounter when using technology.

Key Stage 2

Children will have appropriately supervised access to age-appropriate online tools, search facilities and resources that support planned learning. They will be taught increasingly independent strategies for safe and responsible use of technology, including how to evaluate online information, protect personal information and report concerns.

7.2 Managing Internet Access

- Access to academy internet and IT systems will be provided in accordance with the user's role, age and educational need.
- Staff and visitors who are provided with access to academy IT systems, resources or internet services will be required to understand and follow the relevant Acceptable Use Policy.
- Children's internet access will be appropriately supervised and restricted according to their age, developmental stage and educational needs.
- Appropriate filtering and monitoring systems will be in place to help protect children from harmful and inappropriate online content.
- All staff will understand that filtering and monitoring systems alone cannot safeguard children. Effective supervision, professional vigilance and age-appropriate online safety education remain essential.
- Staff will know how to report concerns about inappropriate content, blocked or accessible websites, or the effectiveness of filtering and monitoring systems.
- Access to inappropriate or harmful online content will be managed in accordance with the academy's safeguarding and online safety procedures.

7.3 Filtering and Monitoring



The Saints Academies will provide filtering and monitoring systems that are appropriate to the age and needs of its children and reflect the academy's safeguarding responsibilities. Filtering and monitoring arrangements will meet the current DfE Filtering and Monitoring: Core Standard.

7.3.1 Decision Making and Oversight

- The leadership team and Local Academy Council (LAC) will ensure that appropriate filtering and monitoring systems are in place.
- A named member of the Senior Leadership Team and a named member of the LAC will have responsibility for ensuring that the DfE Filtering and Monitoring Standards are met.
- The DSL will understand the filtering and monitoring systems and processes in place and their role in safeguarding children.
- Filtering and monitoring provision will be reviewed at least annually by appropriate members of the leadership team, DSL, IT support and responsible LAC member.
- The review and any resulting actions will be formally recorded.
- Appropriate checks of filtering and monitoring systems will take place throughout the academic year and will be recorded.
- Filtering and monitoring arrangements will be reviewed when significant changes are made to academy technology, systems, devices or internet provision, including the introduction of generative AI tools.
- Decisions regarding filtering and monitoring will be informed by safeguarding risk assessments and the age, developmental stage and needs of the children.
- The academy will seek to avoid unreasonable over-blocking which may unnecessarily restrict appropriate teaching and learning.

7.3.2 Filtering

- Internet access will be provided through the academy's approved internet and filtering provision.
- Filtering will seek to prevent access to illegal, inappropriate and harmful online content.
- The academy will ensure that its filtering arrangements include appropriate protection against access to known child sexual abuse material, including use of the Internet Watch Foundation (IWF) URL list where applicable.
- Filtering arrangements will be regularly maintained and reviewed to ensure that they remain effective, appropriate and proportionate.
- Staff will not attempt to bypass or disable filtering systems unless specifically authorised for legitimate technical purposes.

If a child or member of staff encounters inappropriate or harmful online content:

- The concern will be reported promptly to an appropriate member of staff and, where relevant, the DSL.



- Relevant information, such as the website or URL, will be recorded where this can be done safely and without accessing or reproducing illegal content.
- The concern will be referred to technical support where appropriate so that filtering arrangements can be reviewed.
- Safeguarding concerns will be recorded and escalated in accordance with the academy's Child Protection and Safeguarding Policy.
- Parents and carers will be informed where appropriate.
- Suspected illegal content will be managed and reported in accordance with safeguarding procedures and advice from appropriate agencies.

7.3.3 Monitoring

- Users will be informed that use of academy IT systems and internet services may be monitored for safeguarding, security and appropriate-use purposes.
- Monitoring will be carried out lawfully, proportionately and in accordance with data protection and privacy requirements.
- Monitoring arrangements will be appropriate to the academy's context and the age and needs of its children.
- Appropriate staff will understand how monitoring information and alerts are received, reviewed and escalated.
- Safeguarding concerns identified through monitoring will be reported promptly to the DSL and managed in accordance with safeguarding procedures.
- Monitoring arrangements and their effectiveness will be reviewed at least annually and following significant changes to technology or identified risks.
- The LAC will receive appropriate information to provide oversight and assurance that filtering and monitoring arrangements are effective.

7.4 Security and Management of Information Systems

The Saints Academies will take appropriate measures to protect the security of its information, systems, networks and devices.

These will include:

- Keeping operating systems, applications, antivirus and other security software appropriately updated.
- Using appropriate security measures to protect against malware and other cyber threats.
- Protecting personal and confidential data through appropriate encryption and secure systems.
- Ensuring portable storage devices are only used where authorised and are appropriately checked and protected.



- Preventing the installation of unauthorised software on academy devices.
- Ensuring staff do not open suspicious links, downloads or email attachments.
- Providing individual user accounts and appropriate access permissions.
- Using multi-factor authentication where appropriate and available.
- Requiring users to lock or log out of devices when they are left unattended.
- Regularly reviewing access to academy systems and removing access when it is no longer required.
- Ensuring security incidents and suspected data breaches are reported promptly in accordance with academy procedures.
- Undertaking appropriate reviews and checks of security arrangements.

7.4.1 Passwords and Account Security

All members of staff will have their own individual account and password for systems where individual access is required.

Users will:

- Use strong and appropriately secure passwords.
- Keep passwords and authentication information private.
- Not share individual accounts with other users.
- Not log in using another person's individual account.
- Use multi-factor authentication where required.
- Keep authentication devices and codes secure.
- Report suspected compromise of an account or password promptly.
- Lock or log out of systems when they are not in use.

Where shared or class accounts are necessary for young children, these will be appropriately managed by staff and will not provide children with unnecessary access to personal or confidential information.

7.5 Managing the Safety of our Website

- Information published on academy websites will meet relevant Department for Education requirements and comply with data protection, accessibility, privacy, copyright and intellectual property requirements.
- Personal information about children and staff will not be published unless there is a clear and lawful reason to do so.



- Children's images, videos and work will only be published in accordance with academy procedures and appropriate parental consent arrangements.
- Contact information published on the website will use appropriate academy contact details rather than personal staff or pupil contact information.
- Administrator access to academy websites will be appropriately secured and restricted to authorised users.
- Appropriate safeguarding and online safety information will be made available through academy websites.
- Staff responsible for publishing content will remain aware that images, video, audio and other online content can potentially be copied, altered, manipulated or misused, including through artificial intelligence and deepfake technology.
- Any concerns about inappropriate, fraudulent or impersonated online content relating to the academy, staff or children will be reported promptly to the leadership team and/or DSL and appropriate action will be taken.

7.6 Publishing Images and Videos Online

The Saints Academies recognises the importance of protecting children's privacy, dignity and safety when photographs, videos or other digital content are created or shared.

- Images and videos of children will only be taken, stored, used and published for legitimate academy purposes and in accordance with data protection requirements, academy policies and parental consent arrangements.
- Only academy-approved devices will be used by staff to take photographs or videos of children.
- Staff will not use personal mobile phones, cameras or other personal devices to photograph or record children.
- Images and videos will be stored securely and only accessed by authorised users.
- Staff will consider the content and context of an image before publication and will not publish images that could reasonably place a child at risk, cause embarrassment or compromise their dignity.
- Children's personal information will not be unnecessarily associated with published images or videos.



- Staff will be aware that images, video and audio published online may potentially be copied, altered or manipulated, including through AI and deepfake technology.
- Any suspected misuse, manipulation or unauthorised sharing of images of children will be reported promptly to the DSL and managed as a safeguarding concern where appropriate.

7.7 Managing Email

Access to and use of academy email systems will be in accordance with data protection requirements, confidentiality expectations, Acceptable Use Policies and the Staff Code of Conduct.

- Staff will use their academy-provided email account for official academy business and will not use personal email accounts for communication involving children, parents/carers or confidential academy information.
- Sensitive or personal information will only be communicated using approved and appropriately secure systems.
- Staff will remain vigilant to phishing, fraudulent emails, suspicious links, attachments and other online scams and will report concerns in accordance with academy procedures.
- Staff will not open unexpected or suspicious attachments or links.
- Spam, phishing and suspicious emails will be reported through appropriate academy procedures.
- Academy email addresses and other official contact details will not be used to create personal social media or other unrelated personal accounts.
- Offensive, threatening or inappropriate communications received through academy systems will be reported to the appropriate member of the leadership team and/or DSL.
- Staff will maintain professional boundaries when communicating electronically with parents, carers and children.
- Staff are encouraged to maintain an appropriate work-life balance when responding to electronic communications, including email and approved parent communication systems.

7.8 Management of Applications (Apps) Used to Record Children's Progress

The Saints Academies may use approved digital systems and applications to record, assess and share children's learning and progress.

The Executive Headteacher is ultimately responsible for ensuring that systems used to process children's personal information are appropriately assessed and used in accordance with UK GDPR, the Data Protection Act 2018 and academy data protection procedures.

To safeguard children's information:



- Only academy-approved systems and applications will be used to record or store children's personal information, attainment, observations, photographs or videos.
- Systems will be appropriately assessed before use, including consideration of safeguarding, privacy, security and data protection.
- Staff will only use academy-issued or specifically authorised devices to access systems containing children's personal or sensitive information.
- Personal staff devices will not be used to take, store or upload photographs, videos, observations or other personal information about children.
- Access will be restricted to authorised users and protected by appropriate passwords and other security measures.
- Devices used to access children's information will be appropriately secured, particularly when taken off site.
- Parents and carers who are provided with access to children's learning or assessment information will be informed of expectations regarding privacy, security and appropriate use.
- Parents and carers must not share access details or publish photographs, videos or information relating to other children obtained through academy systems.
- Any suspected unauthorised access, loss, disclosure or misuse of children's information will be reported promptly in accordance with safeguarding and data protection procedures.

7.9 Emerging Technologies and Artificial Intelligence (AI)

The Saints Academies recognises that artificial intelligence (AI), generative AI and other emerging technologies can provide educational and administrative opportunities but may also present safeguarding, privacy, accuracy, bias and data protection risks.

The academies will take an age and developmentally appropriate approach to the use of AI and emerging technologies.

Use with Children

- AI tools will only be used with children where they have been approved by the academy and considered appropriate for the children's age, developmental stage and educational needs.
- Children will not be expected to independently access generative AI tools that are not designed or approved for their age group.
- Use of AI with children will be appropriately supervised by an adult.
- Children will be taught, in an age-appropriate way, that AI-generated information, images or other content may not always be accurate or true.



- Children will be encouraged to ask a trusted adult if they are unsure or concerned about AI-generated or other digital content.

Staff Use

- Staff will only use AI and generative AI tools for academy purposes where their use is consistent with academy policies and procedures.
- Staff must not enter identifiable children's personal information, photographs, safeguarding information, assessment information, confidential information or other sensitive data into public or unapproved AI tools.
- AI-generated information will not be assumed to be accurate. Staff remain professionally responsible for checking the accuracy, suitability and appropriateness of content before it is used.
- Staff will consider potential bias, misinformation, inappropriate content and copyright or intellectual property issues when using AI-generated material.
- AI-generated content will not replace professional judgement, particularly in relation to safeguarding, assessment or decisions about individual children.

Approval and Review

- New AI tools and emerging technologies will be appropriately assessed before being introduced for academy use, including consideration of educational benefit, age appropriateness, safeguarding, privacy, security and data protection.
- The academy will have regard to relevant DfE guidance and safety standards when considering the use of generative AI products.
- Staff will receive appropriate information and training about the safe and responsible use of AI and emerging technologies.
- The LAC will receive appropriate information to support its oversight of safeguarding risks associated with AI and emerging technologies.
- The academy's approach to AI and emerging technologies will be reviewed regularly as technology, guidance and associated risks develop.

8. Social Media

8.1 Expectations

The Saints Academies recognises that social media, messaging services, online games and other platforms that enable users to communicate and share content can provide opportunities but may also present safeguarding and online safety risks.



For the purposes of this policy, social media includes social networking sites, blogs, forums, video and photo-sharing platforms, messaging services, online games with communication features and other online services that allow users to communicate or share content.

All members of The Saints Academies community are expected to use social media and online communication in a safe, respectful and responsible manner.

- Online behaviour that is threatening, abusive, discriminatory, harmful, defamatory or otherwise inappropriate will not be tolerated.
- Personal or confidential information about children, families, staff or the academy must not be shared inappropriately online.
- Online safety concerns involving social media or online communication will be reported to the DSL and/or leadership team and managed in accordance with relevant safeguarding, behaviour, anti-bullying and staff conduct procedures.
- The academy will respond to safeguarding concerns involving social media or online communication whether they occur on or off academy premises where they may affect the safety or welfare of a child or member of the academy community.

8.2 Staff Personal Use of Social Media

The Saints Academies recognises that staff may use social media in their personal lives. Staff must ensure that their online behaviour remains consistent with the professional standards expected of them. Expectations regarding safe and professional use of social media will be included within staff induction, the Staff Code of Conduct, Acceptable Use Policies and relevant safeguarding training.

Staff will:

- Maintain appropriate professional boundaries when using personal social media accounts.
- Consider carefully the information, opinions, photographs, videos and other content they publish or share online.
- Ensure that their personal use of social media does not bring the academy or their professional role into disrepute.
- Take appropriate steps to protect the privacy and security of their personal accounts.
- Be aware of privacy settings, location-sharing features and the potential for online content to be copied, shared or made public regardless of privacy settings.
- Ensure that personal views are not presented as those of The Saints Academies.
- Never share or discuss confidential information obtained through their employment, including information, photographs or videos relating to children, families or colleagues.
- Report to the leadership team any online content or communication that may conflict with their professional role or raise a safeguarding concern.



Communication with Children and Parents/Carers

- Staff will not use personal social media accounts, profiles or personal messaging services to communicate with children.
- Staff will not add, follow or accept current pupils as contacts or "friends" through personal social media accounts.
- Staff will not use personal social media accounts to communicate with parents or carers in relation to academy business.
- Communication with parents and carers regarding academy matters will take place through academy-approved communication systems.
- If a child, parent or carer attempts to contact a member of staff through their personal social media account regarding academy matters, the member of staff will maintain professional boundaries and report the contact to the leadership team where appropriate.
- Any safeguarding concern arising from online contact will be reported immediately to the DSL.

8.3 Children's Use of Social Media, Messaging and Online Communication

The Saints Academies recognises that its children are aged 3-9 and that many social media platforms and online services have minimum age requirements above the age of children attending the academies.

The academies will not create or require children to create accounts for social media platforms or online services that are not appropriate for their age.

Children will receive age and developmentally appropriate education about social media, online games, messaging and other forms of online communication.

Teaching will focus on helping children to understand that:

- They should only use apps, games, websites and online services that are appropriate for their age and with the knowledge and supervision of a parent, carer or trusted adult.
- Some games and online services allow people to communicate with them through messages, voice or chat functions.
- People they encounter online may not always be who they say they are.
- Personal information, photographs and videos should not be shared online without permission from a trusted adult.
- They should behave kindly and respectfully towards others when using technology.
- They should not respond to messages or contact that makes them feel worried, uncomfortable, confused or unsafe.
- They should tell a trusted adult if someone they do not know tries to contact them online or asks them to share personal information, photographs or videos.



- They should tell a trusted adult if they see or experience something online that worries, frightens, upsets or confuses them.
- They can ask a trusted adult for help to block or report inappropriate contact or content.

Concerns about a child's use of social media, messaging, online games or other communication services will be managed in accordance with the academy's safeguarding and behaviour procedures and will be discussed with parents or carers where appropriate.

9. Use of Personal Devices and Mobile Phones

The Saints Academies recognises that personal devices, including mobile phones, smart watches, tablets and other connected or wearable technology, are part of everyday life. However, their use within the academies must not compromise the safeguarding of children, professional conduct, privacy, data protection or the security of academy information.

9.1 Staff Use of Personal Devices and Mobile Phones

Staff are expected to model safe, responsible and professional use of technology.

- Personal mobile phones and devices must be kept securely and should not normally be used while staff are supervising or working directly with children.
- Personal devices may only be used during appropriate breaks or in designated staff areas, except where there is an agreed professional, emergency or medical reason for their use.
- Staff must not use personal mobile phones, cameras, smart watches or other personal devices to photograph, video or record children.
- Photographs, videos and recordings of children must only be made using academy-approved devices and systems.
- Staff must not store children's personal information, photographs, videos, observations, assessment information or other confidential academy information on personal devices.
- Staff must not use personal phone numbers, personal messaging accounts or personal social media accounts to communicate with children.
- Communication with parents and carers about academy matters must take place through academy-approved communication systems.
- Staff must ensure that personal devices do not automatically connect, upload, synchronise or back up academy information, photographs or recordings to personal accounts or cloud storage.
- Staff must take appropriate steps to secure any personal device that is authorised to access academy systems.



- Personal devices must not be used in a way that distracts staff from the effective supervision and safeguarding of children.

Any breach of these expectations will be reported to the Executive Headteacher or appropriate senior leader and managed in accordance with the Staff Code of Conduct and relevant safeguarding or disciplinary procedures.

9.2 Visitors, Volunteers and Contractors

Visitors, volunteers and contractors will be expected to use personal devices in a way that does not compromise the safety, privacy or wellbeing of children.

- Personal mobile phones and devices should be kept securely and should not normally be used in areas where children are present.
- Visitors, volunteers and contractors must not photograph, video or record children unless this has been specifically authorised by the academy for an agreed purpose.
- Any authorised photography or recording must be undertaken using arrangements approved by the academy.
- Visitors must follow any additional instructions provided by academy staff regarding the use of mobile phones, cameras, smart watches or other connected devices.

Concerns about the inappropriate use of a personal device by a visitor, volunteer or contractor will be reported immediately to the Executive Headteacher and/or DSL.

9.3 Children's Personal Devices

Due to the age of children attending The Saints Academies, children do not normally need to bring personal mobile phones or other internet-enabled personal devices into the academy.

Where a child needs to bring a mobile phone or other personal device for an agreed reason:

- This must be agreed with the academy and parent/carer.
- The device must be switched off and stored securely in accordance with academy arrangements during the school day.
- Children will not normally be permitted to use personal mobile phones or internet-enabled devices during the school day.
- The academy accepts no responsibility for the loss of or damage to personal devices brought onto academy premises, except where responsibility arises under applicable law.
- Any inappropriate use of a personal device will be addressed in accordance with the academy's safeguarding, behaviour and online safety procedures.

Where a child uses a smart watch or other wearable device, the academy may require functions such as messaging, calling, photography, recording or internet access to be disabled during the school day. The academy reserves the right to restrict or prohibit the use of personal devices where their use presents a safeguarding, privacy, behaviour or learning concern.



9.4 Searching, Examining or Confiscating Devices

Where there are concerns regarding a child's personal device, staff will act in accordance with current Department for Education guidance, academy behaviour procedures and safeguarding procedures. Staff will not routinely search the content of a child's personal device.

Where there is reason to believe that a device may contain evidence of a safeguarding concern, harmful content or prohibited material, the matter will be referred promptly to the Executive Headteacher and/or DSL.

If there is concern that a device may contain nude or semi-nude images of a child, staff must **not intentionally view, copy, print, share, forward, save or otherwise distribute the imagery**. The matter must be referred immediately to the DSL and managed in accordance with the academy's safeguarding procedures and current UKCIS guidance.

9.5 Allegations and Safeguarding Concerns Involving Personal Devices

Any allegation or safeguarding concern relating to a member of staff's use of a personal device will be reported and managed in accordance with the academy's Child Protection and Safeguarding Policy, Staff Code of Conduct and procedures for managing allegations or concerns about adults working with children. Where a concern relates to a child, the DSL will consider the child's age, developmental stage, individual circumstances and any additional vulnerabilities when determining the appropriate safeguarding response. Parents and carers will be informed where appropriate, unless doing so would place a child at increased risk or conflict with safeguarding advice.

10. Responding to Online Safety Incidents and Concerns

The Saints Academies will ensure that all members of the academy community understand how to report online safety concerns and that concerns are responded to promptly, appropriately and in accordance with safeguarding procedures.

Online safety concerns may include, but are not limited to:

- Access to harmful, inappropriate or illegal online content.
- Concerning online contact or communication.
- Cyberbullying or harmful online behaviour.
- Inappropriate sharing of personal information, images or videos.
- Concerns arising through social media, messaging services or online games.
- Online grooming, exploitation or coercion.
- Financial scams, phishing or other online fraud.
- Misuse of academy technology, systems or accounts.



- Concerns relating to artificial intelligence (AI), including AI-generated or manipulated images, videos, audio or other content.
- Concerns about filtering, monitoring or security systems.
- Online behaviour which may indicate a wider safeguarding concern.

10.1 Reporting Concerns

All staff have a responsibility to report online safety concerns.

- Any concern about a child's safety or welfare online must be reported promptly to the Designated Safeguarding Lead (DSL) or a Deputy DSL.
- If the DSL or Deputy DSL is unavailable, staff must not delay taking appropriate safeguarding action.
- Staff will follow the academy's Child Protection and Safeguarding Policy and established safeguarding reporting procedures.
- Children will be encouraged to tell a trusted adult whenever something online makes them feel worried, frightened, uncomfortable, confused or unsafe.
- Children will not be blamed or punished for reporting something that has happened to them online.
- Parents and carers will be encouraged to report online safety concerns to the academy.
- Concerns involving the conduct of a member of staff, volunteer, contractor or other adult working with children will be managed in accordance with the academy's procedures for allegations and concerns about adults.

Where there is an immediate risk of harm, appropriate action will be taken without delay, including contacting emergency services or other relevant safeguarding agencies where necessary.

10.2 Responding to Concerns

When responding to an online safety concern, the DSL and/or appropriate senior leader will consider:

- The nature and seriousness of the concern.
- The child's age and developmental stage.
- Any additional needs or vulnerabilities.
- Whether other children may be at risk.
- Whether the incident indicates abuse, exploitation, bullying, grooming or another safeguarding concern.
- Whether the content or behaviour may be illegal.
- Whether parents or carers should be informed and involved.
- Whether advice or support is required from children's social care, the police or another relevant agency.
- Whether technical action is required, such as reviewing filtering, monitoring, accounts or access arrangements.
- Whether additional education or pastoral support is required.



The response will be proportionate to the circumstances and focused on safeguarding and supporting the child.

10.3 Recording Online Safety Concerns

Online safety incidents that raise safeguarding concerns will be recorded in accordance with the academy's safeguarding procedures.

Records should include, where appropriate:

- A clear summary of the concern.
- When and how the concern was reported.
- The children and/or adults involved.
- Actions taken.
- Decisions made and the reasons for those decisions.
- Advice sought from other agencies where applicable.
- Communication with parents or carers where appropriate.
- The outcome and any follow-up action required.

Records will be stored securely and confidentially in accordance with safeguarding and data protection requirements.

Patterns or repeated incidents will be monitored by the DSL and used to inform safeguarding practice, staff training, curriculum planning and future online safety education.

10.4 Preserving Evidence

Where an online safety incident may require further safeguarding or police involvement, staff will seek advice from the DSL before taking action that could remove or alter potential evidence.

Staff must not intentionally view, copy, print, download, save, forward or share illegal imagery or suspected child sexual abuse material.

Where a concern involves nude or semi-nude imagery of a child, staff will follow the specific procedures within this policy and current safeguarding guidance.

Staff should record relevant information, such as usernames, dates, times, platform names or web addresses, where it is safe and appropriate to do so without accessing, copying or reproducing illegal material.

10.5 Informing Parents and Carers

Parents and carers will normally be informed of online safety concerns involving their child and will be supported to help keep their child safe.

However, the DSL may decide that parents or carers should not be informed immediately where doing so could:

- Place the child or another person at increased risk of harm.



- Interfere with a safeguarding or police investigation.
- Lead to the loss or destruction of evidence.
- Otherwise be contrary to the child's best interests.

Where necessary, the DSL will seek advice from children's social care, the police or another appropriate safeguarding agency before contacting parents or carers.

10.6 Review Following an Incident

Following a significant online safety incident, the academy will consider whether any changes are required to:

- Safeguarding procedures.
- Filtering and monitoring arrangements.
- Technology or system access.
- Risk assessments.
- Staff training.
- Online safety education.
- Acceptable Use Policies.
- Parental information or support.

Lessons learned will be used to strengthen future safeguarding and online safety practice.

11. Online Sexual Violence and Sexual Harassment

The Saints Academies recognises that sexual violence and sexual harassment can occur online as well as offline and that online technology may be used to facilitate or extend harmful sexual behaviour.

Online sexual harassment may include, but is not limited to:

- Sexualised comments, messages or language.
- Unwanted sexualised contact or communication.
- Sharing sexualised images or videos.
- Pressuring another person to share an image, video or information.
- Sexualised bullying.
- Sharing or displaying inappropriate sexual content.
- Making or sharing sexualised, altered or manipulated images, including content created using artificial intelligence (AI) or deepfake technology.
- Other online behaviour of a sexual nature that causes or may cause harm, distress or concern.

11.1 Age and Developmental Considerations



The Saints Academies recognises that children attending the academies are aged 3-9 and that any concerning or sexualised behaviour must be considered in the context of the child's age, developmental stage, understanding and individual circumstances.

Staff will not assume that a young child understands the sexual meaning or significance of their behaviour.

Where concerning or developmentally inappropriate sexual behaviour occurs, staff will consider whether it may indicate:

- Curiosity or behaviour that requires appropriate education and boundaries.
- Exposure to inappropriate online or offline content.
- Imitation of behaviour or language the child has seen or heard.
- A need for additional support or education.
- Harmful behaviour from another child.
- Grooming, coercion or exploitation.
- Abuse or other safeguarding concerns.

All concerns will be considered carefully and referred to the DSL where appropriate. The child's age will never be used as a reason to dismiss a safeguarding concern.

11.2 Responding to a Concern

The Saints Academies has a zero-tolerance approach to sexual violence and sexual harassment. Concerns will never be dismissed as "banter", "just having a laugh", "part of growing up" or otherwise normalised.

Where staff become aware of online sexual violence, sexual harassment or concerning sexualised behaviour, they will:

- Respond calmly and take the concern seriously.
- Reassure the child that they have done the right thing by telling a trusted adult.
- Avoid asking leading or unnecessary questions.
- Report the concern promptly to the DSL or Deputy DSL.
- Make an accurate safeguarding record in accordance with academy procedures.
- Avoid intentionally viewing, copying, saving, forwarding or sharing sexual imagery involving children.
- Preserve relevant information or evidence safely where appropriate, without reproducing illegal or harmful material.
- Follow the academy's Child Protection and Safeguarding Policy.

The DSL will consider the immediate safety and wellbeing of all children involved and determine what further action is required.



11.3 Safeguarding Response

The DSL will consider each concern on a case-by-case basis, taking into account:

- The age and developmental stage of the child or children involved.
- The nature and context of the behaviour.
- Any difference in age, developmental stage, power or vulnerability.
- Whether the behaviour appears consensual, coercive, threatening or exploitative.
- Whether there is evidence of pressure, manipulation or grooming.
- Whether the behaviour has occurred previously or forms part of a pattern.
- Any SEND, communication needs or other vulnerabilities.
- Whether online content or contact may have influenced the behaviour.
- Whether any child is at immediate risk of harm.
- Whether a referral to children's social care, the police or another agency is required.

The academy's response will be child-centred, proportionate and focused on safeguarding all children involved.

11.4 Supporting Children

Children affected by online sexual violence, sexual harassment or concerning sexualised behaviour will be provided with appropriate support.

The academy will:

- Ensure that children feel listened to and taken seriously.
- Avoid language that blames or shames a child.
- Consider appropriate pastoral and educational support.
- Consider whether changes to supervision or arrangements are required to keep children safe.
- Work with parents and carers where appropriate.
- Seek support from external safeguarding professionals or agencies where necessary.

Where another child is responsible for harmful behaviour, that child will also be considered in need of appropriate safeguarding, education and support. Any behaviour or disciplinary response will be considered alongside the child's age, developmental stage and safeguarding needs.

11.5 Parents and Carers

Parents and carers will normally be informed of concerns involving their child unless there is a safeguarding reason not to do so.



Where informing a parent or carer may place a child at increased risk, interfere with an investigation or otherwise be contrary to safeguarding advice, the DSL will seek advice from children's social care, the police or another appropriate agency before making contact.

11.6 Education and Prevention

The Saints Academies will provide age and developmentally appropriate education which supports children to understand:

- Appropriate personal boundaries.
- Respectful and kind behaviour towards others.
- That their body belongs to them.
- That they can say no to unwanted or uncomfortable behaviour.
- That photographs and personal information should not be shared without appropriate permission.
- That they should tell a trusted adult if something they see, hear or experience online or offline makes them feel worried, uncomfortable, confused or unsafe.
- That they will be listened to and supported when they ask for help.

This learning will be reinforced through appropriate Relationships Education/RSE, PSHE, Computing, safeguarding education and everyday academy practice.

12. Sharing Nudes and Semi-Nudes

The Saints Academies recognises that incidents involving the sharing of nudes and semi-nudes are safeguarding concerns and must be responded to in accordance with the academy's Child Protection and Safeguarding Policy and current UK Council for Internet Safety (UKCIS) guidance.

For the purposes of this policy, 'sharing nudes and semi-nudes' refers to the sending or posting of nude or semi-nude images, videos or live streams involving children under the age of 18. This may take place through social media, messaging services, gaming platforms, chat applications, forums or between devices.

The term may include images that have been created, altered or manipulated using technology, including artificial intelligence (AI).

12.1 Age and Developmental Considerations

The Saints Academies recognises that its children are aged 3-9.

Any incident involving nude or semi-nude imagery will therefore be considered carefully in the context of the child's age, developmental stage, understanding, individual circumstances and any additional vulnerabilities.



Staff will not assume that a young child understands the sexual nature, meaning or potential consequences of an image or behaviour.

An incident involving a young child may indicate:

- Accidental or unintentional sharing.
- Age-related curiosity.
- Exposure to inappropriate content.
- Imitation of something the child has seen or experienced.
- Inappropriate contact from another person.
- Pressure, coercion or grooming.
- Harmful sexual behaviour.
- Sexual abuse or exploitation.
- Another safeguarding concern.

The child's young age will never be used as a reason to dismiss a concern.

12.2 Initial Response

If an incident involving a nude or semi-nude image, video or live stream comes to the attention of a member of staff:

- The incident must be reported to the DSL or Deputy DSL as soon as possible.
- Staff should respond calmly and reassure the child that they have done the right thing by telling an adult.
- Staff should not blame, shame or punish a child for making a disclosure.
- Staff should not ask unnecessary or leading questions.
- Staff should not investigate the incident themselves.
- Staff should not intentionally view, copy, print, download, save, forward, share or otherwise distribute the imagery.
- Staff should not ask a child to show them the imagery.
- Staff should not photograph or screenshot the imagery.
- The device should be handled in accordance with safeguarding procedures and advice from the DSL.
- An accurate safeguarding record should be made in accordance with academy procedures.

Where there is concern that a child has been harmed or is at immediate risk of harm, the DSL will make an immediate referral to children's social care and/or the police as appropriate.

12.3 DSL Response



The DSL will undertake an initial review of the incident with appropriate members of staff and determine the appropriate safeguarding response.

The DSL will consider:

- The age and developmental stage of the child or children involved.
- What is known about the image or content without unnecessarily viewing it.
- How the image was created and shared.
- Whether the image was created voluntarily or whether pressure, coercion, grooming or manipulation was involved.
- Whether the image has been shared with other people or more widely online.
- Whether an adult is involved.
- Whether there is a significant age or developmental difference between those involved.
- Whether the child has SEND, communication needs or other vulnerabilities.
- Whether the incident forms part of a pattern of concerning behaviour.
- Whether there are concerns about sexual abuse, exploitation or harmful sexual behaviour.
- Whether AI or other technology has been used to create or manipulate an image.
- Whether another child may be at risk.
- Whether children's social care and/or the police should be contacted.

The primary concern at all times will be the welfare and protection of the child or children involved.

12.4 Viewing Imagery

Staff should not normally view nude or semi-nude imagery involving a child.

In exceptional circumstances, the DSL may decide that viewing an image is necessary to support safeguarding decision-making. Any decision to view imagery must be made in accordance with current UKCIS guidance.

Where viewing is considered necessary:

- The decision must be discussed with the Executive Headteacher or an appropriate senior leader.
- Viewing must be undertaken by the DSL or another appropriately authorised member of the safeguarding team.
- Another member of staff should be present.
- Viewing should take place on academy premises wherever possible.
- The image must not be copied, printed, downloaded, saved, shared or forwarded.
- The reason for viewing, who was present and any subsequent action must be recorded in the child's safeguarding record.



If there is any concern that the imagery may constitute child sexual abuse material or that an adult may be involved, staff must not view the imagery and advice should be sought from the police and/or children's social care.

12.5 Parents and Carers

Parents and carers will normally be informed at an early stage and involved in supporting their child. Parents and carers will not be informed where there is good reason to believe that doing so may place the child at increased risk of harm.

Where there is uncertainty, the DSL will seek advice from children's social care, the police or another appropriate safeguarding agency before contacting parents or carers.

The academy will support parents and carers to respond calmly and appropriately and to prioritise the child's safety and wellbeing.

12.6 Recording Incidents

All incidents involving the sharing of nudes and semi-nudes will be recorded as safeguarding concerns.

Records will include, where appropriate:

- The nature of the concern.
- How and when it came to the academy's attention.
- The children and/or adults involved.
- The outcome of the DSL's initial review.
- Decisions made and the reasons for those decisions.
- Whether imagery was viewed and, if so, why and by whom.
- Advice sought from other agencies.
- Referrals made.
- Communication with parents or carers.
- Support provided to the child.
- Any follow-up action required.

The imagery itself must not be copied or stored within the child's safeguarding record.

12.7 Reporting and Removal

Where imagery has been shared online, the DSL will consider appropriate reporting and removal routes and seek advice from relevant safeguarding agencies where necessary.

The academy will not place responsibility on a child to manage the removal of harmful or illegal imagery without appropriate adult support.



Where an adult is suspected of creating, possessing, requesting or sharing sexual imagery involving a child, this will be treated as a potential child sexual abuse concern and referred to the appropriate safeguarding agencies without delay.

12.8 Supporting Children

The academy's response will prioritise the welfare and safeguarding of all children involved.

Children will:

- Be listened to and taken seriously.
- Be reassured that they have done the right thing by telling a trusted adult.
- Be supported without blame or shame.
- Receive age and developmentally appropriate support.
- Be helped to understand appropriate boundaries and safe image sharing.
- Receive additional pastoral or safeguarding support where necessary.

Where another child has been involved in creating or sharing imagery, their behaviour will also be considered in the context of their age, developmental stage and safeguarding needs.

12.9 Education and Prevention

Due to the age of children attending The Saints Academies, education will focus on the underlying principles of safe and appropriate image sharing rather than explicitly teaching young children about the sharing of nudes and semi-nudes.

Through age and developmentally appropriate Relationships Education/RSE, PSHE, Computing and safeguarding education, children will be supported to understand:

- That their body belongs to them.
- Appropriate personal boundaries.
- That photographs and videos should only be taken or shared appropriately.
- That they should ask a trusted adult before sharing photographs or personal information online.
- That it is not acceptable for someone to pressure them to take or share a photograph.
- That they should tell a trusted adult if someone asks them to take, send or look at a photograph that makes them feel worried, uncomfortable, confused or unsafe.
- That they can always ask a trusted adult for help.

Teaching will be sensitive, non-alarmist and appropriate to children's age, developmental stage and readiness.

13. Online Child Sexual Abuse and Exploitation



The Saints Academies recognises that technology and the internet may be used to facilitate child sexual abuse and exploitation. This may occur through websites, social media, messaging services, online games, live-streaming services or other online platforms.

Online child sexual abuse and exploitation may involve an adult or another child and can include:

- Building a relationship with a child online in order to groom, manipulate or exploit them.
- Encouraging or pressuring a child to engage in sexualised conversation or behaviour.
- Asking a child to create, view or share sexual images or videos.
- Sending a child sexual or otherwise inappropriate content.
- Using threats, pressure, rewards, gifts or manipulation to influence a child's behaviour.
- Encouraging a child to keep online communication or activity secret from trusted adults.
- Arranging or attempting to arrange offline contact with a child.
- Recording, sharing or live streaming abusive or exploitative content.
- Creating, altering or manipulating sexualised images of a child, including through artificial intelligence (AI) or deepfake technology.

13.1 Age and Developmental Considerations

The Saints Academies recognises that children aged 3–9 may not understand that online contact or behaviour is inappropriate, abusive or exploitative.

Young children may:

- Believe that a person they communicate with online is who they claim to be.
- Not recognise inappropriate questions, requests or behaviour.
- Be encouraged to keep communication secret.
- Respond to attention, praise, rewards or offers within games or online services.
- Accidentally share personal information, photographs or videos.
- Find it difficult to explain what has happened or why something has made them uncomfortable.

Staff will therefore remain alert to changes in a child's behaviour, language, play, emotional wellbeing or use of technology that may indicate exposure to inappropriate online content, contact or experiences.

A child's age or apparent lack of understanding will never be used as a reason to dismiss a safeguarding concern.

13.2 Indicators of Concern

Possible indicators of online abuse or exploitation may include:

- A child becoming unusually secretive about their use of technology.
- A child becoming worried, upset or distressed after using a device or going online.



- Unexpected knowledge, language or behaviour that appears inappropriate for the child's age or developmental stage.
- A child referring to an online "friend" or person that adults do not know.
- Receiving unexpected messages, requests, gifts or rewards through online games or services.
- A child being asked to keep online activity or communication secret.
- A child expressing fear or anxiety about a particular person, game, app or device.
- Sexualised behaviour or language that raises concern.
- Unexplained changes in behaviour or emotional wellbeing.

The presence of one indicator does not necessarily mean that abuse or exploitation has occurred. Staff should consider the child's individual circumstances and report concerns in accordance with safeguarding procedures.

13.3 Responding to Concerns

Any concern that a child may be experiencing online sexual abuse, grooming or exploitation must be treated as a safeguarding concern.

Staff will:

- Listen carefully and calmly to the child.
- Reassure the child that they have done the right thing by telling a trusted adult.
- Avoid blaming or shaming the child.
- Avoid asking leading or unnecessary questions.
- Not investigate the concern themselves.
- Report the concern immediately to the DSL or Deputy DSL.
- Make an accurate safeguarding record in accordance with academy procedures.
- Preserve relevant information where it is safe and appropriate to do so without accessing, copying or sharing illegal material.

Where imagery is involved, staff will follow the procedures set out in **Section 12 – Sharing Nudes and Semi-Nudes**.

The DSL will assess the concern and make referrals to children's social care, the police or other appropriate safeguarding agencies where required.

Where a child is believed to be at immediate risk of harm, action will be taken without delay.

13.4 Illegal Images and Child Sexual Abuse Material

Staff must not intentionally search for, view, copy, print, download, save, forward or share suspected child sexual abuse material.



If suspected illegal material is encountered accidentally:

- Staff should stop viewing the content.
- The content must not be copied, downloaded, saved or shared.
- The concern must be reported immediately to the DSL.
- Staff should follow the DSL's instructions regarding the device and preservation of relevant information.
- The DSL will seek appropriate advice and make any necessary referral or report to the relevant safeguarding or law enforcement agency.

Staff should not attempt to investigate illegal content themselves.

13.5 Supporting Children

Children who may have experienced online abuse, grooming or exploitation will be treated as children in need of safeguarding and support.

The academy will:

- Prioritise the child's immediate safety and wellbeing.
- Listen to and take the child's concerns seriously.
- Avoid language or responses which could blame or shame the child.
- Provide appropriate pastoral and safeguarding support.
- Consider the child's age, developmental stage, SEND, communication needs and other vulnerabilities.
- Work with parents and carers where appropriate.
- Work with external safeguarding professionals and agencies where necessary.
- Consider whether additional measures are required to protect other children.

13.6 Education and Prevention

Due to the age of children attending The Saints Academies, education will focus on simple, age and developmentally appropriate protective messages rather than explicit teaching about sexual exploitation.

Children will be supported to understand:

- That they can tell a trusted adult if anything online worries, frightens, confuses or upsets them.
- That they should not share personal information, photographs or videos without checking with a trusted adult.
- That people online may not always be who they say they are.
- That they should tell a trusted adult if someone they do not know tries to contact them.
- That they should tell a trusted adult if someone asks them to keep online communication secret.



- That they should tell a trusted adult if someone asks them to do, say, look at or share something that makes them uncomfortable.
- That they will be listened to and supported when they ask for help.

These messages will be reinforced through age-appropriate Relationships Education/RSE, PSHE, Computing, online safety education and everyday safeguarding practice.

14. Cyberbullying

The Saints Academies recognises that bullying can take place online as well as face-to-face.

Cyberbullying may occur through messaging services, social media, online games, websites, shared images or videos, or other digital technology.

Cyberbullying may include:

- Sending unkind, upsetting, threatening or intimidating messages.
- Deliberately excluding someone from an online group or activity.
- Sharing embarrassing, private or personal information, photographs or videos without permission.
- Posting or sharing unkind or harmful comments about another person.
- Impersonating another person online.
- Using online games, messaging or other technology to repeatedly upset, frighten or target another person.
- Creating, altering or sharing harmful or humiliating content about another person, including content created or manipulated using artificial intelligence (AI).

14.1 Age and Developmental Considerations

The Saints Academies recognises that children aged 3-9 may have different levels of understanding about online communication, friendship, privacy and the impact of their behaviour on others.

Children may not always understand that something they consider funny or playful may upset or harm another person.

Staff will respond to incidents in a way that takes account of the child's age, developmental stage, understanding, individual needs and the nature of the behaviour.

Online behaviour will not automatically be classified as bullying following a single incident. The academy will consider the circumstances, including whether behaviour is repeated or forms part of a pattern, while recognising that a single online incident may still be serious and require safeguarding or behaviour action.

14.2 Responding to Cyberbullying



Cyberbullying concerns will be taken seriously and managed in accordance with the academy's Behaviour Policy, Anti-Bullying Policy and Child Protection and Safeguarding Policy, as appropriate.

Staff will:

- Listen to and reassure the child reporting the concern.
- Report safeguarding concerns promptly to the DSL.
- Record incidents in accordance with academy procedures.
- Avoid unnecessarily viewing, copying or sharing harmful content.
- Preserve relevant information safely where this may be required as evidence.
- Consider whether other children may be affected or at risk.
- Work with parents and carers where appropriate.

Where cyberbullying occurs outside the academy but affects a child's wellbeing, relationships or safety within the academy, appropriate action will be taken in accordance with academy policies and safeguarding procedures.

14.3 Supporting Children

The academy will provide appropriate support for children affected by cyberbullying.

Where a child has displayed harmful or bullying behaviour online, the academy will also consider their age, understanding and safeguarding needs and provide appropriate education, support and consequences.

The aim will be to:

- Keep children safe.
- Stop harmful behaviour.
- Support children who have been affected.
- Help children understand the impact of their actions.
- Restore positive and respectful relationships where appropriate.
- Reduce the likelihood of further incidents.

14.4 Education and Prevention

Children will receive age and developmentally appropriate education about respectful and responsible behaviour when using technology.

Children will be taught to:

- Be kind and respectful when using technology.
- Understand that words and actions online can affect other people's feelings.
- Ask permission before sharing photographs or information about someone else.
- Not join in with unkind or upsetting online behaviour.



- Tell a trusted adult if something online makes them or someone else feel worried, upset, frightened or uncomfortable.
- Ask a trusted adult for help rather than trying to deal with an online problem by themselves.

These messages will be reinforced through PSHE, Relationships Education/RSE, Computing, online safety education and the academy's wider approach to positive behaviour and relationships.

15. Online Hate, Radicalisation and Extremism

The Saints Academies recognises that children may encounter harmful online content which promotes hatred, discrimination, extremist views or radicalisation.

Online hate may include content or communication that targets a person or group because of characteristics such as race, religion, disability, sex or other protected characteristics.

The Saints Academies will treat concerns relating to online hate, radicalisation and extremism as safeguarding concerns and will respond in accordance with the academy's Child Protection and Safeguarding Policy and Prevent responsibilities.

15.1 Age and Developmental Considerations

The Saints Academies recognises that children aged 3–9 may encounter harmful or inappropriate ideas online without understanding their meaning, purpose or potential impact.

Young children may repeat words, phrases, views or behaviours they have seen or heard online without fully understanding them.

Staff will consider:

- The child's age and developmental stage.
- The context in which the language, behaviour or concern has arisen.
- Whether the child has been exposed to inappropriate or harmful online content.
- Whether another person may be influencing the child.
- Whether the behaviour is repeated or forms part of a wider pattern.
- Any additional needs or vulnerabilities.
- Whether the concern indicates a wider safeguarding risk.

A child's age or lack of understanding will not prevent staff from reporting a concern where there may be a safeguarding risk.

15.2 Responding to Concerns



Staff will remain alert to online content, communication or behaviour that may indicate exposure to hate, extremist material or radicalising influences.

Where a concern is identified, staff will:

- Respond calmly and appropriately.
- Avoid challenging or questioning a child in a way that could compromise a safeguarding response.
- Report the concern promptly to the DSL or Deputy DSL.
- Record the concern in accordance with academy safeguarding procedures.
- Not investigate suspected extremist or illegal online material themselves.
- Follow the academy's Child Protection and Safeguarding Policy and Prevent procedures.

The DSL will assess the concern and consider whether further advice, support or referral is required in accordance with current safeguarding and Prevent procedures.

Where appropriate, the DSL will work with parents and carers and relevant external agencies.

15.3 Online Hate and Discriminatory Behaviour

Online hate, discriminatory language and harmful online behaviour will not be tolerated.

Where children encounter or display discriminatory or hateful content or behaviour, the academy will consider both:

- The impact on any child who has been targeted or affected; and
- The age, understanding, circumstances and safeguarding needs of the child displaying the behaviour.

Appropriate safeguarding, educational, pastoral and behaviour support will be provided.

15.4 Education and Prevention

Online safety education will be appropriate to children's age and developmental stage.

Children will be supported to:

- Treat other people with kindness and respect, both online and offline.
- Understand that it is not acceptable to be unkind to someone because they are different.
- Recognise, at an age-appropriate level, that not everything they see or hear online is true or trustworthy.
- Understand that some online content may try to influence what people think or believe.
- Tell a trusted adult if they see or hear something online that worries, frightens, confuses or upsets them.



- Know that they can always ask a trusted adult for help.

These messages will be reinforced through age-appropriate PSHE, Relationships Education/RSE, Computing, online safety education, collective worship and the academy's wider work to promote respect, inclusion and positive relationships.

Signed: *Karen Mann* Chair of LAC

Signed: *Rebecca Walker* Executive Headteacher