Online Safety Policy, including Filtering & Monitoring Policy and Use of Artificial Intelligence (AI) in School Policy

At St Paul's CofE Primary School & Nursery, our vision is *Learning in God's Love*. We believe that everyone is loved and valued by God, and we strive to help all members of our community grow in courage and compassion. Children are encouraged to reach their full potential and flourish as they learn together within a caring and inclusive community.

Our vision is theologically rooted in the words of St Paul's letter to the Corinthians:

"Stand firm in the faith; be courageous; be strong. Let all that you do be done in love."
(1 Corinthians 16:13–14)

This vision underpins our approach to online safety. We recognise that technology and the online world are an important part of modern life and provide many opportunities for learning, creativity and communication. At the same time, we understand the responsibility we have to teach children how to navigate the digital world safely, responsibly and compassionately.

Guided by the example of Jesus — who taught the importance of kindness, wisdom, honesty and treating others with dignity — we encourage children to use technology in ways that reflect our values of Courage, Compassion and Community. We want children to understand that their actions online should reflect the same care and respect they show to others in person.

Through education, support and clear expectations, we aim to develop confident and responsible digital citizens who are able to make safe choices online, communicate respectfully and seek support when needed. We work in partnership with children, families, staff and the wider community to create a culture where everyone understands the importance of online safety and responsible technology use.

Scope of the Online Safety Policy

This Online Safety Policy sets out how St Paul's CofE Primary School & Nursery will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, Children, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, St Paul's CofE Primary School & Nursery will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Policy development, monitoring and review

This policy has been developed by the senior leadership and safeguarding team, whilst also drawing on the expertise and responsibilities across the school. Membership includes:

- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governors
- Parents/carers

Consultation within the school community has taken place through a range of formal and informal opportunities to ensure the policy is understood, workable and proportionate.

Schedule for approval, monitoring and review

Reviewed and updated: August 2026

Approval: Governing Body

Next scheduled review: August 2027

Monitored by: Leadership and Safeguarding Team

Monitoring frequency: Annually

Reporting to the Governing Body: Annually

Policy review cycle: reviewed annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Children, Parents/carers, Staff

Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with governors, the DSL and IT provider on filtering and monitoring.

Governors

Governors approve the Online Safety Policy and challenge its effectiveness, in line with KCSIE expectations.

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with DfE standards.
- Undertake basic cyber security awareness training and support school cyber security oversight.

Governors also support parent/carer and community engagement in online safety.

Designated Safeguarding Lead (DSL)

KCSIE states the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information, confirming at least annual checks.
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for Children with SEND.

Online Safety Lead (OSL)

The OSL will:

- Support the Leadership and Safeguarding Team with day-to-day online safety oversight and support the DSL.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSL/OSL to implement the school's separate Online Safety Curriculum Strategy, which sets out the planned and progressive curriculum from EYFS to Year 6. The strategy is delivered primarily through ProjectEVOLVE and is reinforced through Teach Computing, PSHE/RSHE, other relevant curriculum areas, assemblies and pastoral provision, and whole-school awareness activity including Safer Internet Day and Anti-Bullying Week.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the DSL
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Children

Children will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices.

Community users

Community users accessing school systems or platforms will sign a Community User AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

Online Safety Oversight

Online safety oversight at St Paul's sits within the Leadership and Safeguarding Team rather than a separate standing committee. The team monitors implementation and impact of this policy and ensures online safety is embedded across safeguarding, curriculum and technical practice, drawing on governor, IT, staff, pupil and parent/carer input where appropriate.

Membership

- DSL, OSL, Senior Leader(s)
- Online Safety Governor
- IT/technical representative (internal or provider)
- Staff representatives (teaching/support)
- Pupil voice, where appropriate
- Parent/carer feedback, where appropriate

Core responsibilities

The group supports the DSL/OSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from Children, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions (e.g. 360 safe).

Governance and impact

- Oversight arrangements, responsibilities and reporting lines are reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside the Safeguarding and Child Protection Policy, Relationship, Behaviour and Anti-Bullying Policy, Data Protection Policy and the separate Online Safety Curriculum Strategy.

What the policy does

- Defines responsibilities for online safety.
- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes Children's digital competence and critical understanding.

Implementation, monitoring and review

- Developed and reviewed through the Leadership and Safeguarding Team at least annually, and sooner if risks or technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 safe, ProjectEVOLVE).
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to Children and parents/carers through AUAs and awareness activity.
- Published on the school website.

Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs) *(see appendices)*. AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and children induction/handbooks
- on-screen reminders (e.g. splash screens), digital signage
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website
- peer support / learner-led activity

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • *Note: follow UKSIC and UKCIS*					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	guidance when responding to self-generated intimate images (SGII).					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission *Incidents will be assessed by senior leaders and the DSL. Suspected criminal activity or serious safeguarding concerns will be referred to the police or other appropriate agency where required. Where suitable, preventative or diversionary support may also be considered.*					X
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

	Staff and other adults				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)	x				x			
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*				x	x			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)		x					x	
Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*	x				x			

Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*			x		x			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*			x		x			
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*			x		x			
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds)*			x		x			
Personal mobile phones used for learning (teacher-directed and supervised)	x				x			
Personal mobile phones used during social time/breaks (where permitted) including device-free approaches			x		x			
Taking photos/video/audio on personal devices (including sharing, location data and consent)	x				x			
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*	x				x			
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*	x				x			
School email used for personal communication (non-work/non-learning)			x		x			
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*	x				x			

Reporting and responding

Introduction

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in s

and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Pupils may report a concern to any trusted adult, including the DSL team. Staff must report safeguarding concerns promptly to the DSL and record them on MyConcern in line with the school's safeguarding procedures. Parents/carers and other members of the community may report concerns directly to the school through the published safeguarding contact routes.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

The school will:

- Maintain secure and confidential records of online safety incidents, actions, decisions and follow-up. Safeguarding concerns are recorded on MyConcern in accordance with the school's safeguarding procedures; technical and filtering/monitoring records are retained through the relevant secure systems.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - The Leadership and Safeguarding Team
    - Senior leaders
    - Governors (via safeguarding reports)
    - *Staff*
    - *Children, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners where relevant*

External Support and Escalation

The school will work with appropriate external agencies when required, including:

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- *UK Safer Internet Centre's Professionals Online Safety Helpline*
- *Reporting Harmful Content service*

School actions

Most incidents will involve inappropriate rather than illegal use. St Paul's will respond promptly and proportionately, using the Safeguarding and Child Protection Policy, Relationship, Behaviour and Anti-Bullying Policy, Staff Code of Conduct and disciplinary procedures as appropriate. Where behaviour outside school causes harm, disruption or distress within the school community, the school may respond where this is consistent with its safeguarding and behaviour responsibilities. Suspected criminal or serious safeguarding matters will be escalated to the appropriate external agency.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of Children and staff remains central to our approach.

Policy statements

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping Children understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear v

- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and Children, including ensuring Children's work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to DSL
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support Children in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

Education

Online Safety Education Programme

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school's planned, progressive and inclusive programme of online safety education is set out in the separate Online Safety Curriculum Strategy. It is aligned to nationally recognised guidance and frameworks, including DfE "Teaching Online Safety in Schools", UKCIS "Education for a Connected World" and SWGfL ProjectEVOLVE. Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas including RSHE/RSE, Health Education and Computing, with assessment and clear intended outcomes.

The programme develops Children's ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;

- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).

Where internet use is planned, Children are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, age-appropriate pupil voice and feedback, and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities.

Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include:
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured CPD
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through:

- Attendance at training offered by the Local Authority, MAT or other relevant organisations (e.g. SWGfL).
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of Children. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving Children in sharing online safety messages with parents/carers, including contributing to information events.

- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

Technology

Purpose

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Detailed arrangements are set out in the Appendix C1 - Filtering and Monitoring Policy Template and Appendix C2 - Technical Security Policy Template.

Filtering and Monitoring

St Paul's uses Smoothwall for filtering and monitoring across the school's managed digital environment. Smoothwall supports the school in protecting users from illegal, inappropriate and harmful online content and activity, alongside staff supervision, safeguarding procedures and professional judgement. The provision is configured and reviewed with the school's IT provider in line with KCSIE, the DfE filtering and monitoring standards and UK Safer Internet Centre guidance.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and Children understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering)
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Further detail is provided in the Appendix C1 - Filtering and Monitoring Policy

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and receive appropriate assurance
- staff and Children are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation.

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration.

Further detail is provided in the Data Protection Policy

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Technology Practice

Purpose

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in *Keeping Children Safe in Education*, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice and education.

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, Children and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education

Decisions about device use are informed by risk assessment and reviewed regularly.

At St Paul's, pupils must not bring or use personal mobile phones, gaming devices or other personal smart technology in school unless prior agreement has been given by the Headteacher for a specific reason, for example independent travel. Where a phone is permitted, it must be switched off on arrival, handed to the class teacher or other designated member of staff for secure storage, and returned at the end of the school day. Unauthorised use will be dealt with proportionately under the Relationship, Behaviour and Anti-Bullying Policy; a device may be confiscated and returned to a parent/carer where appropriate. Smartwatches, earbuds and other connected personal devices are subject to the same expectations unless specifically authorised.

Digital Content

The school recognises that digital content (images, video and any other multi-modal digital media) can enrich learning and communication when used responsibly. It directly supports KCSIE expectations around sexual imagery, sharing of images, consent and coercion. It also reinforces lawful management of digital content as part of safeguarding and embeds education and prevention alongside policy.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and Children are trained/educated to understand their responsibilities when creating or sharing digital content

- personal data and images are handled securely and lawfully
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and Children, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)

- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, Children and parents
- national guidance and statutory expectations

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, Children and parents/carers. Evaluating student outcomes related to online safety should be defined and incorporated into the school's assessment processes. Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

List of appendices

The appendices are as follows:

A2 - Learner Acceptable Use Agreement – KS2
A3 - Learner Acceptable Use Agreement– for younger Children (EY/KS1)
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement
A8 - Harmful Sexual Behaviour Policy
A10 - Responding to incidents of misuse – flow chart
C1 – Filtering and Monitoring Policy
C5 - Electronic Devices - Searching Screening and Confiscation Policy
C7 – Use of Artificial Intelligence (AI) in Schools Policy

Appendix A2 - Acceptable Use Agreement – for KS2 Children

This acceptable use agreement is intended:

- to ensure that Children will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help Children understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I agree to use the school's digital systems safely and responsibly to protect me, other Children and the school.

Be **Ready** – Be **Safe** – Be **Kind**

Keeping Safe Online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules?

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: _____Group/Class:_____

Signed: _____Date: _____

_____

Parent/Carer Counter signature .....

Appendix A3 - Acceptable Use Agreement – for younger Children (EY/KS1)

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school!

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

Signed (child): _____

Signed (parent): _____

Date _____

Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people , both within schools and in their lives outside school. The internet

are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal e

images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with Children and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the Children, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
  - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal

data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Appendix A8 - Harmful Sexual Behaviour Policy

Purpose

The school recognises that harmful sexual behaviour may be happening but not reported and that it increasingly occurs online involving image sharing, coercion, exploitation and anonymous abuse.

The purpose of this policy is to set out the school's approach to preventing, identifying and responding to Harmful Sexual Behaviour (HSB), sexual harassment and sexual violence between children.

This policy forms part of the school's safeguarding framework and should be read alongside other relevant policies.

The school adopts a zero-tolerance approach to harmful sexual behaviour in line with national safeguarding guidance (see list below)

Scope

This policy applies to:

- All Children, staff, volunteers and governors
- Behaviour occurring within and outside school where it impacts the school community

Legislative and National Context

This policy reflects national guidance including:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children (DfE)
- Violence Against Women and Girls (VAWG) strategy (UK Government)
- Ofsted Review of Sexual Abuse in Schools and Colleges.
- Sharing Nudes and Semi-Nudes: Advice for Education Settings

Roles and Responsibilities

- Governors provide strategic oversight, ensure annual review of this policy and monitor safeguarding trends.
- Senior Leaders promote a culture of respect and equality and ensure consistent implementation and staff training.
- The Designated Safeguarding Lead (DSL) leads responses to incidents, ensures safeguarding procedures are followed, completes risk assessments and liaises with external agencies.
- All staff must challenge inappropriate behaviour, report concerns immediately to the DSL and respond to disclosures in a calm and supportive manner.

Policy Statement

The school will ensure that:

- A whole-school safeguarding approach is taken to preventing harmful sexual behaviour
- All reports are taken seriously and responded to promptly
- Victims are supported, believed and protected

- Children displaying harmful behaviour receive appropriate safeguarding and educational support
- Incidents are managed in line with safeguarding and statutory procedures
- Patterns and trends are monitored to inform prevention strategies

Prevention and Education

The school will ensure that:

- High-quality Relationships and Sex Education (RSE) is delivered
- Children are taught about consent, respectful relationships and healthy boundaries
- Online safety education addresses digital sexual abuse, coercion and image-based harm
- Sexist language, misogyny and harmful gender stereotypes are actively challenged
- Children are encouraged to be positive bystanders and report issues they see
- Reporting systems are accessible, appropriate and clearly communicated

Reporting and Responding

The school will ensure that:

- Multiple reporting routes are available and understood
- All incidents are recorded securely in line with safeguarding and data security procedures
- Risk assessments are completed where appropriate
- The safety and wellbeing of those affected is prioritised
- External specialist agencies are involved where required
- Criminal matters are referred to the police where appropriate

Support and Risk Management

The school will ensure that:

- Victims receive appropriate pastoral and safeguarding support
- Children displaying harmful behaviour receive proportionate and educational intervention
- Risk assessments are dynamic and regularly reviewed
- Supervision and safety planning are proportionate and protective

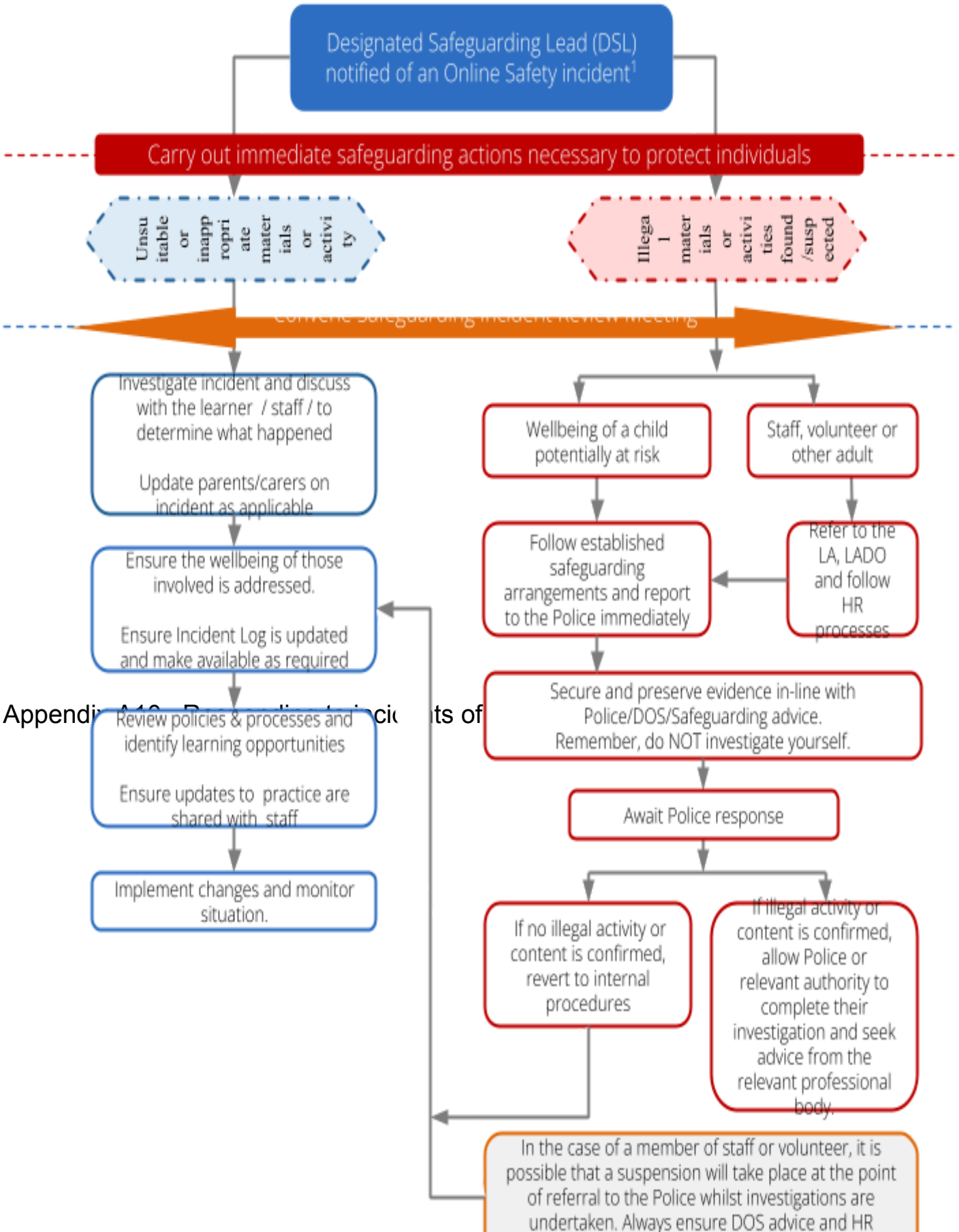
Online Harmful Sexual Behaviour

Online incidents will be managed in line with DfE guidance and may involve specialist reporting services where appropriate.

Training and Review

The school will ensure that:

- DSLs receive specialist safeguarding training
- All staff receive regular safeguarding updates
- Governors receive appropriate oversight training
- This policy is reviewed annually and updated in response to legislative changes or emerging risks



Appendi A10 – Responding to incidents of

Blank Page

Appendix C1 – Filtering and Monitoring Policy

Purpose

The purpose of this policy is to ensure that appropriate filtering and monitoring systems are in place to safeguard Children and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. St Paul's uses Smoothwall as its filtering and monitoring solution. Filtering and monitoring form part of the school's wider safeguarding responsibilities and are implemented in line with Keeping Children Safe in Education (KCSIE) and the DfE filtering and monitoring and technical standards.

Scope

This policy applies to:

- All users of the school's IT systems
- All school-owned devices
- Any device accessing the school's network or internet connection
- Filtering and monitoring provided through third-party or managed services

Roles and Responsibilities

- Governors provide strategic oversight and assurance that filtering and monitoring standards are met.
- Senior leaders ensure appropriate systems are in place, reviewed and resourced.
- The DSL leads safeguarding responses arising from filtering or monitoring alerts.
- The IT service provider maintains the school's Smoothwall filtering and monitoring provision and provides reports, technical support and configuration changes as agreed with the school.
- All staff report concerns relating to access, alerts or system effectiveness.

Policy Statement

The school will ensure that:

- Internet access is filtered to block illegal, harmful and inappropriate content
- Monitoring systems are in place to identify safeguarding concerns and enable timely intervention
- Filtering and monitoring are proportionate, transparent and risk-based
- Roles and responsibilities are clearly defined and understood
- Provision is reviewed regularly and improved in response to risk, practice and guidance

Filtering and monitoring are recognised as supporting safeguarding, not replacing education, supervision or professional judgement.

Filtering

The school will ensure that filtering systems:

- Block access to illegal content, including child sexual abuse material, terrorist material and other unlawful content

- Manage inappropriate and/or harmful content (including search terms and results). These may include:
    - Gambling
    - Hate speech/discrimination
    - Harmful content
    - Mis/Disinformation
    - Piracy and copyright theft
    - Pornography
    - Self-harm and eating disorders
    - Violence against women and girls
- Are age-appropriate and suitable for an educational environment
- Are applied consistently to all users, devices and internet connections, including backup connections
- Allow the identification of individual users and devices in the event of breaches of the filtering policy
- No user should be able to deactivate or bypass systems that filter illegal content.
- Prevent circumvention through VPNs, proxy services or similar technologies
- Support differentiated access for different user groups (e.g. staff and Children)
- Are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning

The school understands the capabilities and limitations of the system and potential impact on implementation and policy is understood.

The school will use recognised tools and guidance to assure the effectiveness of filtering provision e.g., testfiltering.com

Monitoring

The school will ensure that monitoring:

- Enables the identification of safeguarding concerns in a timely manner
- Uses a combination of physical supervision, manual checks and technical systems as appropriate
- Generates alerts that can be prioritised and acted upon by trained staff
- Is subject to human review and professional judgement
- Is clearly communicated to users through policy and acceptable use agreements

Monitoring should be proportionate to the school's risk profile and should not create a culture of surveillance.

Review and Training

Filtering and monitoring provision should be reviewed at least annually and whenever risks or technologies change. Staff, governors and those with specific responsibilities will receive appropriate training.

Appendix C5 – Electronic Devices: Searching, Screening and Confiscation Policy

Purpose

The purpose of this policy is to set out the school's lawful and proportionate approach to searching, screening and confiscating electronic devices and examining or deleting data from those devices.

This policy supports the school's safeguarding responsibilities and must be read alongside the Behaviour Policy, Child Protection and Safeguarding Policy, Online Safety Policy, Filtering and Monitoring Policy, Technical Security Policy and Data Security Policy.

This policy reflects Keeping Children Safe in Education KCSIE), DfE Searching, Screening and Confiscation guidance, DfE Behaviour in Schools guidance and relevant statutory legislation.

Scope

This policy applies to:

- All Children
- All authorised staff
- All electronic devices in a learner's possession
- Devices on school premises or used in connection with school activities
- Behaviour occurring both on and off site where it impacts safeguarding or discipline

Policy Statement

The school will ensure that:

- Searches are lawful, proportionate and necessary
- Safeguarding considerations are prioritised
- Devices are only searched where there are reasonable grounds
- Deletion of data is undertaken only where there is a lawful and justifiable reason
- Criminal matters are referred to the police
- Incidents are recorded securely
- Staff are appropriately trained

Authorised Staff

- The Headteacher will authorise in writing those staff permitted to conduct searches, examine devices and delete data.
- Authorised staff will receive appropriate training including safeguarding, legal thresholds and digital evidence handling.
- Staff cannot be required to undertake searches.

Screening

Where screening measures are used, they will:

- Be clearly communicated to Children and parents
- Be proportionate and risk-based
- Be implemented consistently
- Support a calm, safe and orderly environment

Searching for Electronic Devices

Electronic devices may be searched with consent or without consent where permitted by legislation. Force will not be used to search for items banned under school rules.

Searches will:

- Be conducted by authorised staff
- Be carried out privately where possible
- Involve removal of outer clothing only
- Not extend to intimate searches

Examination of Electronic Devices

- Staff may examine data where there is a good reason to do so, including where data poses a safeguarding risk or relates to a potential breach of school rules.
- Examination will extend only as far as reasonably necessary to establish the facts.
- Where indecent images of a child are suspected, staff must not intentionally view the image and must refer immediately to the DSL.
- Where material may constitute a criminal offence, the device will be handed to the police.

Deletion of Data

- Data may only be deleted where there is a safeguarding reason and the material is not required as evidence.
- Deletion decisions must be proportionate and recorded.
- Material that may constitute criminal evidence must not be deleted.

Safeguarding Response

All incidents involving device searches will:

- Be referred to the DSL
- Be recorded on MyConcern where the matter is a safeguarding concern, with any related technical or behaviour records completed as required
- Trigger a risk assessment where appropriate
- Involve parents/carers unless doing so would increase risk

Care of Confiscated Devices

The school will ensure secure storage of confiscated devices, documentation of chain of custody and appropriate return procedures.

Training

The school will ensure that:

- Authorised staff receive specialist training
- DSLs understand legal thresholds
- All staff are aware of reporting expectations
- Governors understand oversight responsibilities

Monitoring and Review

The school will maintain records of searches and data deletion, review trends and update this policy annually or in response to national guidance.

Appendix C7 - School Online Safety Policy – Artificial Intelligence in Schools

Policy on the use of Artificial Intelligence in Schools

Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

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

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

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

Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff Discipline policies and codes of conduct
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements
- Curriculum Policies

Policy Statements

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and Children for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

- We will ensure that, within our education programmes, Children understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping Children with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the Children, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, Children and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- *The school will support parents and carers in their understanding of the use of AI in the school*
- *AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support Children to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk*
- *Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.*
- *We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must*

ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Responsibilities

Headteacher and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- Children understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/carers

We work hard to engage parents and carers by:

- *sharing information online e.g., website, social media*
- *providing curriculum information*

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their childrens' learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

Vulnerable groups

We recognise that vulnerable Children are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable Children are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, Children and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties.

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.

    - Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and Children.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing
- PSHE/RSHE
- Cross curricular programmes

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by Children and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- *Learner assessment*
- *Critical evaluation of emerging trends and research findings*
- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Engaging with Children*
- *Staff training*

Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Children Safe."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach Children about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.