



53 Online Safety Policy (Ref MPTOSP)



Mosaic Partnership Trust

53 Online Safety Policy (Ref MPTOSP)

Version 1.0

Policy Approval	Policy Approved	Date of Review
Audit and Risk Committee		



53 Online Safety Policy (Ref MPTOSP)

Contents

1	Scope of the Policy	3
2	Schedule for monitoring and review	3
3	Monitoring the impact of the policy	4
4	Responsibilities	4
5	Online Safety Policy	8
6	Acceptable Use	9
7	Reporting and responding	10
8	Use of Artificial Intelligence (AI)	14
9	Online Safety Education Programme	15
10	Technology	19
11	Technology Practice	22



53 Online Safety Policy (Ref MPTOSP)

1. Scope of the Online Safety Policy

This Online Safety Policy sets out how **St Stephen's Junior School** 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 inform 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 Stephen's Junior School will respond in line with this policy and related procedures, including the school's Safeguarding and Child Protection Policy, Behaviour Policy and the Behaviour Written Statement. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school, that the school becomes aware of.

2. Schedule for approval, monitoring and review

Approved by Trust Management with oversight from the Audit and Risk Committee of the Trustees on: [30 September 2026]

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

Next planned review date: [01 September 2026] (required in KCSIE to be at least annually)

Escalation following serious incidents: the school will inform relevant external agencies as appropriate:

- Area Improvement Lead
- CEO
- Director of Education

And if appropriate:

- LADO
- Police
- Social Care

The Trust has in place a Critical Incident Policy which highlights the approach to any serious incident which would be managed through Business Continuity.



53 Online Safety Policy (Ref MPTOSP)

3. Monitoring the impact of the policy

The Headteacher (school level) and Area Improvement Lead (Trust Level) will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Reviews of the effectiveness of the filtering systems
- Surveys/questionnaires (as appropriate) of: Children, Parents/carers, Staff

4. 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.

4.1 Executive Heads, Headteachers, Heads of School and Senior Leaders

Senior leaders set the culture and ensure that systems are effective. In line with [KCSIE](#), the DSL and Deputy DSLs within the Trust hold 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 in the context of school staff, the CEO in the context of Heads and Centrally deployed staff and the Chair of Trustees in the context of the CEO and Director of Education).
- Ensure that the DSL and Deputy DSL are trained and able to fulfil their roles and responsibilities.
- Have assurance from the IT provider that their staff are trained and able to fulfil their roles in supporting the school/Trust.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports from the IT provider and act on emerging risks and themes, informing the Area Improvement Lead as appropriate.
- Establish a nominated SLT Lead (if not the DSL) to work with the DSL and IT provider on a termly review of the effectiveness on filtering and monitoring systems and ensure that these are recorded



53 Online Safety Policy (Ref MPTOSP)

4.2 Local Governing Committees (LGCs)

LGCs will need to adopt the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards in conjunction with the Headteacher

The LGC Safeguarding Link Governor is the Governor responsible for online safety and therefore they are responsible for:

- Meeting the responsible person for Online Safety at school level whether the DSL or Headteacher if they are fulfilling the DSL role.
- Receive anonymised incident and monitoring summaries on a termly basis
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT and DSL in line with KCSIE and DfE Filtering and Monitoring standards.
- Undertake mandatory basic cyber security awareness training and support school cyber security oversight.
- Governors must also support parent/carers and community engagement in online safety as appropriate.

4.3 Designated Safeguarding Lead (DSL)

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to be explicit in the DSL's job description.

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 Safeguarding Link Governor, the IT provider, the Area Improvement Lead and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.



53 Online Safety Policy (Ref MPTOSP)

- With the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- 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
- 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 the IT provider
- Maintain current knowledge of risks across content, contact, conduct and commerce.

4.5 Curriculum Leads

Curriculum leads will work with the DSL to deliver a planned online safety programme through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. [Safer Internet Day](#).

4.6 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 and Child Protection Policy and the Trust Acceptable Use Policy.
- 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 as age appropriate.
- Challenge harmful online behaviour and report any concerns immediately.
- Use only Trust-approved digital services through the ICT provider, Trust approved 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.



53 Online Safety Policy (Ref MPTOSP)

4.7 IT Service Provider

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

The IT provider will:

- Maintain secure infrastructure and managed user access and provide assurances of this to the Trust and the individual school.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL at school level and the Area Improvement Lead at Trust level
- Monitor systems for misuse and report concerns promptly to the Headteacher at School Level and the Area Improvement Lead at Trust level.
- Follow the Trust's Online Safety policy and keep technical knowledge and training current and up to date.

4.8 Children

Children will:

- Follow the Online Safety Policy (including personal devices where permitted) and the schools Behaviour Policy
- Know who they need to report concerns to.
- Use technology responsibly, respecting others and their copyright and intellectual property with staff supporting this with primary age appropriate language.
- Use AI responsibly and in line with the Trust Policy: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community, including other children and school staff.

4.9 Parents/carers

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

The school will:

- Publish both the Trust Online Safety Policy and the Trust Acceptable Use Policy on the school website.
- Publish the Privacy Notice for Parents and Children
- Provide information guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, letters, newsletters and digital media.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (In line with the Trust Mobile Phone Use Policy).



53 Online Safety Policy (Ref MPTOSP)

4.10 Community Users

Community users should not access school or Trust systems or be given access to school or Trust systems without the written permission of the Chief Executive Officer.

4.11 Safeguarding Welfare and Attendance Group (SWAG)

The Safeguarding Welfare and Attendance Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice.

SWAG Membership

- DSL
- Deputy DSLs (DDSL)
- Senior Leaders that are not the DSL or DDSL

The group supports the DSL to:

- Review and monitor the implementation of the Online Safety Policy and related documents.
- Oversee filtering and monitoring and liaising with the Area Improvement Lead as appropriate.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks and share these with the Area Improvement Lead.
- Gather feedback from learners, staff and parents/carers and take this into account in the context of planning
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions

5. Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding and Child Protection Policy, Behaviour Policy, Trust Behaviour Written Statement and Data Protection policies.

The policy:

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



53 Online Safety Policy (Ref MPTOSP)

Implementation, monitoring and review

The policy:

- is reviewed at least annually (KCSIE Para 121) and sooner if risks technology change.
- is monitored by the DSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity
- findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction, annually and reinforced through training.
- Communicated to children and parents/carers through the Acceptable Use Policy.
- Published on the school website.

6. Acceptable use

Acceptable use is defined through the Online Safety Policy and Acceptable Use Policy. Acceptable Use Policies matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff sign an annual declaration that includes all the policies outlined below
- staff and learner induction makes it a requirement to read the policies outlined below
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- Trust and school website
- peer support / learner-led activity

In the context of the Mosaic Partnership Trust the relevant policies that cover acceptable use and should be read in conjunction with this policy include the:

- Critical Incident Policy (Includes Business Continuity Plan)
- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Mobile Phone Use Policy
- AI Policy
- Data Protection Policy



53 Online Safety Policy (Ref MPTOSP)

7. Reporting and responding

7.1 Introduction

The Trust 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 Trust recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The Trust 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 Trust 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. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child.

7.2 Reporting Concerns

The Trust and its schools will ensure that:

- Clear, accessible reporting routes are in place for all members of the Trust and school community, including pupils, staff, Members, Trustees, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), email contact, or in-person disclosures.
- 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.

7.3 Responding to Concerns

The Trust and its school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The Headteacher, DSL, DDSLs 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 in line with Point 2 and Page 3. 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



53 Online Safety Policy (Ref MPTOSP)

- 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 with support from the IT provider.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

7.4 Recording and Monitoring

The Trust and its school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up that could be subject to scrutiny from the Area Improvement Lead and/or the Chief Executive Officer.
- 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 Area Improvement Lead
 - Senior leaders
 - Trustees and where appropriate local governors
 - Local safeguarding partners where relevant in South Gloucestershire and Wiltshire

7.5 External Support and Escalation

The Trust and its schools will work with appropriate external agencies when required, including:

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

Please refer to the Critical Incident Policy that demonstrates the internal route that the Trust takes with serious incidents.

It is more likely that at school level, schools will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:



53 Online Safety Policy (Ref MPTOSP)

7.6 Responding to Children's Actions

Incidents	Refer to class teacher/tutor	Refer to DSL	Refer to Headteacher	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X	X	X	X					X
Unauthorised access to the school network , including using another person's account or sharing usernames/passwords.	X	X	X					X	
Damaging, corrupting or deleting another user's data.	X	X	X		X	X		X	
Sending offensive, harassing or bullying emails, texts or messages.	X	X	X			X		X	X
Unauthorised downloading/uploading , file sharing or distribution of files.	X	X	X			X		X	X
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	X	X	X		X	X	X	X	X
Failing to report accidental access to offensive or pornographic material	X	X	X		X	X			
Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X	X	X	X	X	X	X
Sharing or receiving content that breaches copyright or data protection law.	X	X	X		X				
Unauthorised use of devices , including taking photos/videos or audio recordings and using a smartphone in school	X	X	X			X			
Unauthorised use of online services (apps, websites or platforms)	X	X	X		X	X	X	X	X
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X	X		X	X	X	X	X
Repeated breaches of these rules following previous warnings or sanctions.	X	X	X		X	X	X	X	X



53 Online Safety Policy (Ref MPTOSP)

7.7. Responding to Staff Actions

Incidents	Refer to line manager	Refer to the Headteacher/DSL	Refer to MAT Area Improvement Lead and the Director of People (HR)	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Professional Expectations and Conduct Policy and Disciplinary Policy
Accessing illegal material (or attempting to), as defined in the earlier “Unsuitable/Inappropriate Activities” section.	x	x	x	x	x	x	x
Breaching data protection or cyber-security requirements , including network security rules.	x	x	x		x	x	x
Accessing offensive or pornographic material (or attempting to).	x	x	x	x	x	x	x
Damaging systems or data , including corrupting/deleting others’ data or deliberately damaging hardware/software.	x	x	x		x	x	x
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	x	x	x		x	x	x
Unauthorised downloading, uploading or file sharing.	x	x	x		x	x	x
Breaching copyright, licensing or intellectual property , including misuse of AI systems.	x	x	x		x	x	x
Unauthorised account/network access , including sharing passwords, using another person’s account, or allowing others access.	x	x	x		x	x	x
Sending offensive, harassing or bullying emails, texts or messages.	x	x	x		x	x	x
Use of personal email/social media/messaging to communicate with children or parents/carers.	x	x	x		x	x	x
Inappropriate personal use of school technology , including personal email and social media use during work time/using school systems.	x	x	x		x	x	x
Mishandling personal data , including storing, displaying or transferring it insecurely.	x	x	x		x	x	x
Any action that undermines professional conduct or a staff member’s professional standing.	x	x	x		x	x	x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x	x		x	x	x
Failing to report incidents , whether accidental or deliberate.	x	x	x		x	x	x
Repeated breaches following previous warnings or sanctions.	x	x	x		x	x	x



53 Online Safety Policy (Ref MPTOSP)

8. 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 and in line with the Trust AI Policy.

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

KCSIE 2026 recognises that children may be subject to harmful online interaction with other users or generative AI applications that simulate these.

The Trust and its schools 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.

8.1 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 as outline in the Trust AI Policy before use.
- Approve tools and accounts. Only Trust-approved AI tools may be used for schoolwork, and staff should use Trust-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 under any circumstances.

8.2 Quality, fairness and integrity

The Trust and its schools 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.



53 Online Safety Policy (Ref MPTOSP)

- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- 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 learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

8.3 Reporting, monitoring and accountability

The Trust and its schools will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the headteacher or in the case of the headteacher, CEO.
- Abide by the AI Policy approved list of AI tools in use.
- Engage parents/carers with clear information about how AI is used in school by sharing the Trust AI Policy on the school website.

8.4 Misuse and disciplinary action

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

Further information regarding use of AI can be found in the trust Artificial Intelligence (AI) Policy.

9. Online Safety Education Programme

9.1 Children

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 delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including [DfE "Teaching Online Safety in Schools"](#), [UKCIS "Education for a Connected World"](#), and resources such as [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, Computing and Citizenship), with assessment and clear intended outcomes.



53 Online Safety Policy (Ref MPTOSP)

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](#)).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

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 will not be temporarily adjusted for curriculum research under any basis.

Pupil voice is actively used to strengthen the Trust and school's approach through feedback, representation and opportunities such as digital leaders (where these exist), peer mentoring and contribution to acceptable use and community-facing online safety activities. Children are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

9.2 Staff and volunteers

In line with [DfE Keeping Children Safe in Education \(KCSIE\)](#), all staff and volunteers receive safeguarding and child protection training through the Trust, 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.
- 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.



53 Online Safety Policy (Ref MPTOSP)

- Staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- Staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- Staff understand and consistently apply the Trust Mobile Phone User Policy requirements, including expectations for their own professional use of personal devices including Smartwatches and Smartglasses.
- Staff follow cyber security policy and requirements.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Policy, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and/or Headteacher (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 professional learning resources (e.g. [ProjectEVOLVE EDU](#)) and, where appropriate, enhanced pathways (e.g. [ProjectEVOLVE SAFEGUARDING](#)).
- Regularly review the implementation of this Online Safety Policy and updates through staff meetings as appropriate.
- Targeted advice, guidance and training from the DSL to individuals as required.

9.3 Trustees and Local Governing Committees (LGCs)

LGCs should take part in online safety training and awareness activity on an annual basis and in line with the Governance Framework. This is particularly important for Trustees serving on the Audit and Risk and Quality of Education Committees alongside the Safeguarding Link Governor and Chair of Governors at a local level.

Training and updates may be provided through:

- Attendance at training offered through Governor Hub 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 between the Safeguarding Link Trustee or Governor with the Area Improvement Lead at Trust level and the Headteacher/DSL at school level.

Enhanced training is mandatory for the Safeguarding Link Governor and Trustee. This will include:

- Basic cyber security awareness training.



53 Online Safety Policy (Ref MPTOSP)

- Discussion with the DSL to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews at school level and with the Area Improvement Lead at a central level.

9.4 External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The Trust recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. The Trust may also draw on external agencies to supplement the Trust's safeguarding approach and has a service level agreement with Melhoria Education in this context and a relationship with South Gloucestershire and Wiltshire Safeguarding teams. The Trust 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 Trust's engagement with external stakeholders:

The Trust 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 and digital communication tools.
- Involving children in sharing online safety messages with parents/carers.
- 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 including the Trust Mobile Phone User Policy.
- Clear communication about the school's mobile-phone arrangements, the reasons for the policy and the consequences of breaches
- Accurate, balanced and age-appropriate information about changes affecting social media and other online services
- Guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- Guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- Providing parents and carers with the school based Safeguarding confidential email.

9.5 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:



53 Online Safety Policy (Ref MPTOSP)

- 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.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies that have an existing partnership with the school (e.g. pre-schools).
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Melhoria Education, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings.

10. Technology

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

10.1 Filtering and Monitoring

The Trust and its schools have appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance through the three IT providers that service the Trust. (e.g., [DfE Technical Standards](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The Trust and its schools ensure that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed with support from the IT providers
- 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 Trust-owned devices are subject to filtering and monitoring, including when used off-site and that staff must only use Trust devices for Trust business.
- 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 Trust.
- where Generative AI products are used through those approved in the AI Policy, they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products



53 Online Safety Policy (Ref MPTOSP)

10.2 Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities at school level, the Trustees and the Area Improvement Lead retain oversight at Trust level.
- The Headteacher at school level and Area Improvement Lead at Trust level will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the Trust in meeting this standard in its schools.
- Filtering and monitoring effectiveness is reviewed at least annually and following significant changes or incidents that go through the Critical Incident Policy. Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead, the Area Improvement Lead and/or CEO depending on the incident and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Records of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- Log reports provide actionable information for safeguarding decisions.
- No system is relied upon in isolation; reporting routes and professional judgement remain central

10.3 Technical Security

The Trust and its Schools will take steps to ensure that its technical infrastructure is secure, reliable and well managed and meet statutory requirements.

The Trust and its schools ensure 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 immediately, 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.

10.4 Cyber Security

The Trust and its schools recognise cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue).

The Trust and its schools ensure that:



53 Online Safety Policy (Ref MPTOSP)

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders, Trustees and governors understand cyber risks and their safeguarding implications 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 in line with the Critical Incident Policy.
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

10.5 Data Protection

The Trust is committed to protecting personal data and complying with data protection legislation in line with the Trust Data Protection Policy. (The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

The Trust ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place. The DPO for Mosaic is Judicium as named in the Data Protection Policy and Privacy Notices.
- 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 including to the ICO as appropriate
- data protection is embedded across safeguarding, teaching, learning and administration
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

10.6 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



53 Online Safety Policy (Ref MPTOSP)

11. Technology Practice

The Trust 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, education and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

11.1 Device Management

The Trust 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 Phone User Policy and explicitly links device use to behaviour, safeguarding and education

The Trust and its schools ensure 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 through the IT provider
- 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 Trust's online safety education
- children do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Behaviour and Mobile Phone User Policies (in line with the DfE statutory guidance)
- staff model the school's requirements and use personal devices only where authorised and professionally appropriate
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

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

11.2 Digital Content

The Trust recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.



53 Online Safety Policy (Ref MPTOSP)

The Trust and its schools ensure 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 educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- Trust-approved platforms and accounts are used where content includes personal or sensitive information
- staff and children understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.

11.3 Public Online Communications

The Trust 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. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse and this is reflected in the AI Policy.

The Trust and its schools ensure that

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the Trust/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 learners, the Trust has procedures in place to control how those images are shared online and images must have the staff and/or child's consent.
- publishing public communications is restricted to authorised and trained staff at Trust and School level.
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts and websites
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

11.4 Review

Technology practice is reviewed regularly to reflect:



53 Online Safety Policy (Ref MPTOSP)

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, children and parents
- national guidance and statutory expectations
- the school's progress towards meeting the DfE digital and technology standards
- the impact of mobile-phone arrangements and changes affecting children's access to online services.