Ramsbury Primary School

Policy Number: S31

ONLINE SAFETY POLICY

Date	Review Date	Coordinator	Nominated Governor
11/26	11/27	Juliet Rean	Helen Foley

This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers and visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

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 of: Learners, parents/carers and staff

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.

Head Teacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with Keeping Children Safe in Education (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, IT provider/technical staff and relevant staff 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.
- 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 the DSL and IT provider, in line with DfE standards.
- Report to the FGB.
- 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 learners with SEND.

Computing Subject Leader

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

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 and sign/comply with the Staff Acceptable Use Agreement (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 / technical staff

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.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy.
- 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 and share the learner AUA.

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 (where permitted in school).

Online Safety Policy

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

The school Online Safety Policy:

- 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 learners' digital competence and critical understanding.
- Is monitored by the DSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 safe, ProjectEVOLVE).
- Is shared at staff induction and reinforced through training.
- Is communicated to learners and parents/carers through AUAs and awareness activity.
- Is 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 learner induction/handbooks
- curriculum and awareness sessions
- communications with parents/carers
- school website
- built into Computing and PSHE lessons

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and 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 guidance when responding to self-generated intimate images (SGII).*					X
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)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using penetration-testing tools without explicit permission					
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	
	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	
	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	

Consideration should be given to the following activities when used for non-educational purposes.	Staff and other adults				Learners			
	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. Twitch, TikTok LIVE, Instagram Live)*	X				X			
Video platforms (YouTube)			X		X			

Personal mobile phones and smart devices on site *(phones, smartwatches without cameras, earbuds)*		X			X			
Mobile phones used for learning (teacher-directed and supervised)	X				X			
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

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 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 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.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), email contact, or in-person disclosures.
- 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 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 a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- 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:
    - Senior leaders
    - Governors (via safeguarding reports)
    - Staff

- Learners, where appropriate
- Parents/carers through general communications
- Local safeguarding partners where relevant

External Support and Escalation

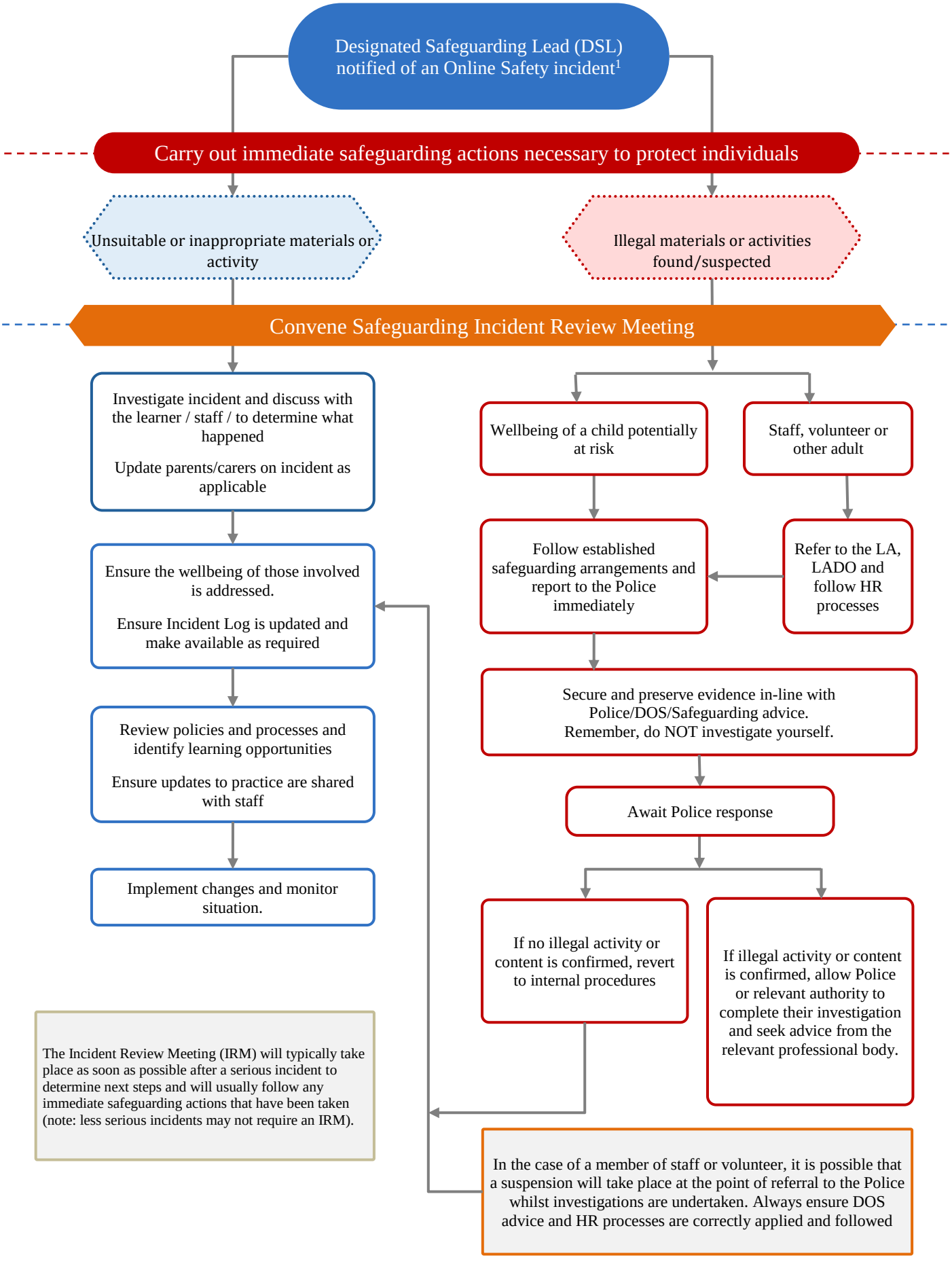
The school will work with appropriate external agencies when required, including:

- 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

Ramsbury Primary School

Policy Number: S31

The school will make the flowchart below available to staff to support the decision-making process.



School actions

It is more likely that the school 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 procedures as follows.

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to DSL	Refer to Head Teacher	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	X	X	X	X
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.		X	X			X			
Damaging, corrupting or deleting another user's data.		X	X			X			
Sending offensive, harassing or bullying emails, texts or messages.		X	X			X		X	X
Unauthorised downloading/uploading, file sharing or distribution of files.		X	X			X			
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).		X	X			X			
Failing to report accidental access to offensive or pornographic material		X	X			X			

Deliberately accessing offensive or pornographic material (or attempting to)		X	X	X	X	X		X	X
Sharing or receiving content that breaches copyright or data protection law.		X	X			X			
Unauthorised use of devices, including taking photos/videos or audio recordings.		X	X			X			X
Unauthorised use of online services (apps, websites or platforms).		X				X			X
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.		X	X			X			X
Repeated breaches of these rules following previous warnings or sanctions.		X	X			X		X	X

Responding to Staff Actions

Incidents	Refer to Head Teacher	Refer to LA DO	Refer to Police	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Staff Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X	X	X	X		X
Breaching data protection or cyber-security requirements, including network security rules.	X					X
Accessing offensive or pornographic material (or attempting to).	X	X	X	X		X
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.	X	X				X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	X				X	
Unauthorised downloading, uploading or file sharing.	X				X	
Breaching copyright, licensing or intellectual property, including misuse of AI systems.	X				X	
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.	X					X
Sending offensive, harassing or bullying emails, texts or messages.	X					X
Use of personal email/social media/messaging to communicate with learners or parents/carers.	X				X	
Inappropriate personal use of school technology, including personal email and social media use	X				X	

during work time/using school systems.						
Mishandling personal data, including storing, displaying or transferring it insecurely.	X				X	
Any action that undermines professional conduct or a staff member's professional standing.	X				X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X					X
Failing to report incidents, whether accidental or deliberate.	X				X	
Repeated breaches following previous warnings or sanctions.	X					X

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 learners and staff remains central to our approach.

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 learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts. Upper Key Stage 2 children will learn about the risks of AI DeepFakes.

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 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.

Reporting, monitoring and accountability

The school will:

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

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 learners 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.
See Ramsbury School AI Policy.

Online Safety Education

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", 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 PSHE and Computing), with assessment and clear intended outcomes.

The programme develops learners' 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, learners are guided to appropriate resources and supported if unsuitable content is encountered. Swiggle is used as a safe search engine whenever possible. 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, learner representation, and opportunities such as 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. Cyber security training takes place annually.
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 through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources.
- Regular review of this Online Safety Policy and updates through staff meetings.
- Targeted advice, guidance and training from the DSL to individuals as required.

Governors

Governors should take part in online safety training and awareness activity, including an annual cyber security training session. 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 or other relevant organisations (e.g. SWGfL).
- Participation in school training and information sessions.
- Regular updates with the DSL at FGB meetings to review key themes, incidents and current priorities.
- Basic cyber security awareness training.

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

- 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 learners. 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 and the school website.
- Offering opportunities such as parent/carer workshops or information events, focused on online safety.
- Involving learners 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.

Technology

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.

Filtering and Monitoring

The school has 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. (e.g., DfE Technical Standards, KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring)

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 learners 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

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 learners 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.

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 in Practice

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. Laptops are used when children are using online search engines to ensure that every child's searches can be monitored through Securus.

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, learners 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.

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 learners 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 learners, the school has procedures in place to control how those images are shared online
- Online safety information is shared with parents and carers
- 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, learners 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, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes (e.g. using ProjectEVOLVE Knowledge Maps assessment and tracking). 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

Mobile technologies

The school allows:

	School devices		Personal devices			
	School owned for individual use	School owned for multiple users	Student owned	Staff owned	Governor owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes	Yes, with agreement with the DSL	Yes, with agreement with the DSL
Full network access	Yes	Yes	No	No	No	No
Access to the Governor SharePoint	Yes	No	No	No	Yes	No
Internet only	Yes	Yes	No	Yes	Yes	Yes

No personal devices should be used around children.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks, including the use of artificial intelligence to manipulate images, attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or in the local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. While the school supports reasonable parental photography for personal use, there may be occasions when temporary restrictions are required. The Headteacher and Senior Leadership Team may introduce temporary restrictions on photography or recording at specific events where safeguarding, child protection, privacy,

copyright, licensing, religious observance, security concerns or exceptional circumstances make such restrictions necessary. Any temporary restrictions will normally be communicated to parents and carers in advance and will be reviewed regularly. Such restrictions may apply to individual events or for a defined period while a safeguarding review or risk assessment is undertaken.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.