



Online Safety Policy

2026-2027

Scope of the Online Safety Policy

This Online Safety Policy sets out how Rampton Primary 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 informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, 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). Roles and responsibilities

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

Policy development, monitoring and review

This policy has been developed by the [Insert group/committee name] (e.g., Online Safety Group), drawing on the expertise and responsibilities across the school. Membership includes: (amend as appropriate)

- Headteacher / Senior leaders
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governors
- Parents/carers
- Community users (where relevant)

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

Policy and Leadership

Responsibilities

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

Headteacher and senior leaders

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

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.

- 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 and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

Governors

Governors approve 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 and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard.

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).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the wider governing body.
- Undertake basic cyber security awareness training and support school cyber security oversight.

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

Designated Safeguarding Lead (DSL)

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.
- With the nominated SLT lead and the IT provider, lead the 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)
- Ensure appropriate support for learners with SEND.

Curriculum Leads

Curriculum leads will work with the DSL to deliver a planned online safety programme through appropriate channels, such as Computing, PSHE/RSE, other curriculum areas, assemblies and national initiatives, such as *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 comply with the staff Acceptable Use Agreement.
- 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, review and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the Headteacher.
- Follow the school's Online Safety policy and keep technical knowledge current.

Learners

Learners will:

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

Parents/Carers

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

The school will:

- Publish the Online Safety Policy and share the learner Acceptable Use Agreement
- Provide guidance on the responsible use of online technologies and seek permission 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).

Community users

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

.

Schedule for approval, monitoring and review

Approved by the Governing Body on: [Insert date]

Monitored by: [Insert name/role/group] e.g. DSL, OSL, SLT

Monitoring frequency: [Insert time period]

Reporting to the Governing Body: [Insert time period] (recommended: at least annually)

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

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

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.

What the policy does

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

Implementation, monitoring and review

- Reviewed at least annually, though sooner if risks/technologies change.
- 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 and reinforced through training.
- Communicated to learners and parents/carers through Acceptable Use Agreements and awareness activity.
- Published on the school website.

Acceptable Use

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

Reinforcement

- Staff and learner induction/handbooks
- Posters in areas where technology is used frequently.
- Curriculum and awareness sessions.
- Communication with parents/carers
- School website
- Peer support/learner-led activity

Acceptable/Unacceptable Actions

18 User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • <i>Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).</i>					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data					

	• Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) ○ Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission <i>Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime and into positive pathways.</i>					
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)					
	Promoting discrimination, harassment or hateful content					
	Using school systems to run a private business or make unauthorised financial gain					
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)					
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)					
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute					

	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)								
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)								
Cloud storage and file sharing (e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents)								
Social media and user-generated platforms (e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services								
Messaging, chat and voice (e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)								
Streaming entertainment/media (video, music, podcasts) e.g. Netflix, Disney+, Spotify								
Video platforms and livestreaming (e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)								
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds). N.b Smartphone bans in schools in England)								
Taking photos/video/audio on devices (including sharing, location data and consent)								
Other personal devices (e.g., tablets, handheld consoles, VR headsets, wearables)								
Personal email accounts on site or on the school network/Wi-Fi (e.g., Gmail, Outlook.com)								
School email used for personal communication (non-work/non-learning)								
Unapproved AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)								

Reporting and responding

Introduction

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keep 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. KCSIE suggests that staff should have a professional curiosity and speak to the Designated Safeguarding Lead (DSL) or deputy if they have concerns about a child.

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.

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:

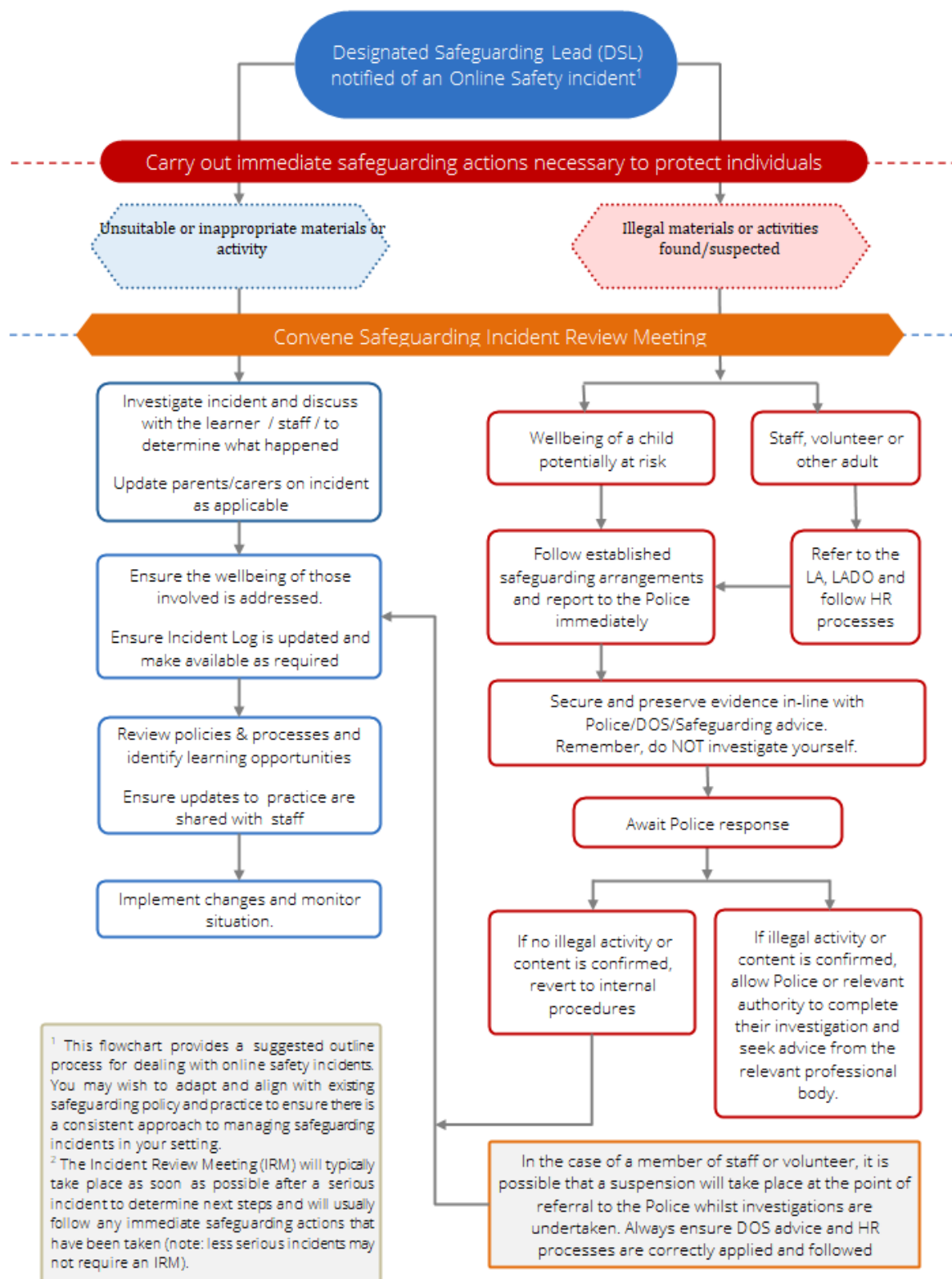
- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
 - Senior leaders
 - Governors (via safeguarding reports)
 - Staff
 - Learners, where appropriate

- Parents/carer 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



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/disciplinary procedures as follows:

[illegible]

[illegible]