



Lee Royd Nursery School

Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) 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).

Version: 1

Date created: 28/09/2026

Next review date: 28/09/2027

Scope of the Online Safety Policy

This Online Safety Policy sets out how [Lee Royd Nursery 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).

Where online safety concerns or incidents occur outside school and are known to the school, [Lee Royd Nursery 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 [Headteacher and Online Safety Governor](#), drawing on the expertise and responsibilities across the school. Membership includes:

- Headteacher
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governor

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.

Schedule for approval, monitoring and review

Approved by the Governing Body on: [19/10/2026](#)

Monitored by: [HT](#)

Monitoring frequency: [Termly](#)

Reporting to the Governing Body: [Annually](#)

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

Next planned review date: September 2027

Escalation following serious incidents: the school will inform relevant external agencies as appropriate, *MAT officers, the Local Authority safeguarding lead, and/or the police.*

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
- Reviews of the effectiveness of the filtering systems
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

Policy and leadership

Responsibilities

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

Headteacher and senior leaders

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

Senior leaders will:

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

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 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 (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 learners with SEND.

Online Safety Lead (OSL)

The OSL will:

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

Teaching and Support Staff

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

Staff will:

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

IT service provider / technical staff

The IT provider Easytech NW LTD – alongside Lancashire County Council supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider Easytech NW LTD 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 *Head Teacher*.
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Online Safety in the Early Years

At Lee Royd Nursery we ensure –

- Children only access the internet under direct adult supervision.
- Online activities are carefully selected and age appropriate.
- Staff support children in learning basic safety messages.
- Children are encouraged to tell an adult if something online worries them.
- Parents are supported through online safety information and newsletters.

- We teach our Golden Rules which is as follows -

This is how we stay safe when we use computers:

- I will ask a grown-up before I use the tablet or computer.
- I will only use the internet when a grown-up is with me.
- I will be gentle with the tablet, keyboard and mouse.
- If I'm not sure, I will ask a grown-up for help.
- If I see something that makes me upset, I will tell a grown-up straight away.
- If I do not follow the rules, I may not be able to use the tablet.

Parents and carers

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

The school will:

- Publish the Online Safety Policy on the school website.
- 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.

What the policy does

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

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually ([KCSIE Para 121](#)), and sooner if risks/technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. [360 safe](#), [ProjectEVOLVE](#)).
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

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

Acceptable use

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

Reinforcement

- staff induction/handbooks
- on-screen reminders (e.g. splash screens), digital signage
- curriculum and awareness sessions
- communications with parents/carers
- school website

Acceptable/Unacceptable Actions

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>					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 & illegal
	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)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	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	

Consider the following activities when used for non-educational purposes. Add or amend items to reflect current technology, age restrictions and your school's device policy.	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. YouTube, Twitch, TikTok LIVE, Instagram Live)	x				x			

Personal mobile phones and smart devices on site (phones, smartwatches, earbuds). <i>N.b Smartphone bans in schools in England</i>			x		X			
Taking photos/video/audio on devices (including sharing, location data and consent)		x			x			
Other personal devices (e.g., tablets, handheld consoles, VR headsets, wearables)	x				x			
Personal email accounts on site or on the school network/Wi-Fi (e.g., Gmail, Outlook.com)	x				x			
School email used for personal communication (non-work/non-learning)	x				x			
Unapproved AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)	x				x			

Reporting and responding

Introduction

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in 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 (or a 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.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools (e.g., Whisper), 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.

Responding to Concerns

The school will ensure that:

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

Recording and Monitoring

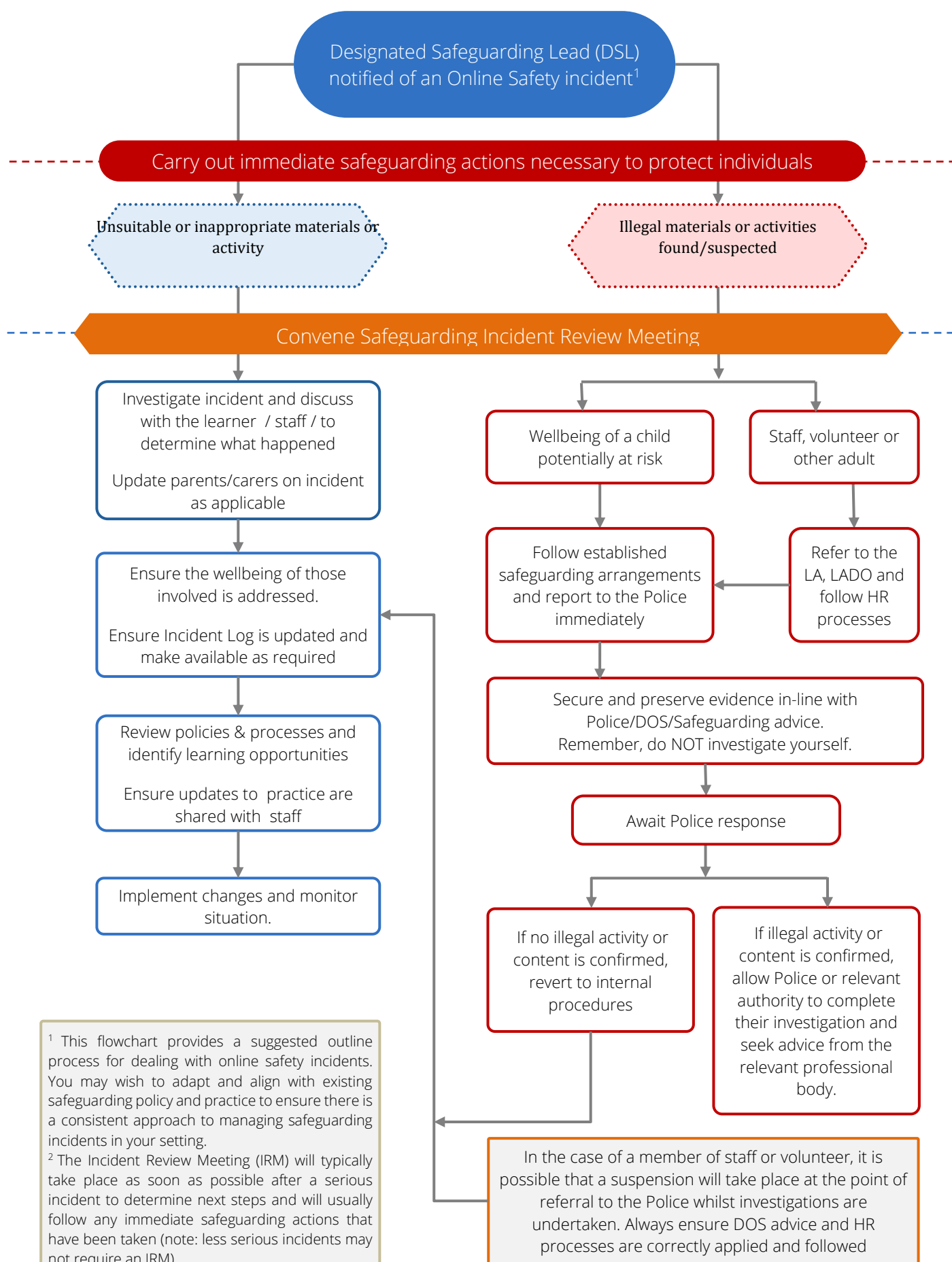
The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Incidents should be logged on CPOMS.
- 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 Online Safety Group
 - 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*



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					
Accessing offensive or pornographic material (or attempting to).		X	X	X			X
Damaging systems or data , including corrupting/deleting others’ data or deliberately damaging hardware/software.		X	X		X		X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).		X	X		X		X
Unauthorised downloading, uploading or file sharing.		X		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	X	
Sending offensive, harassing or bullying emails, texts or messages.		X	X	X			X
Use of personal email/social media/messaging to communicate with learners or parents/carers.		X		X		X	
Inappropriate personal use of school technology , including personal email and social media use during work time/using school systems.		X				X	
Mishandling personal data , including storing, displaying or transferring it insecurely.		X	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			X	X
Failing to report incidents , whether accidental or deliberate.		X				X	
Repeated breaches following previous warnings or sanctions.		X	X			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.

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

Policy statements

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.

- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

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

Quality, fairness and integrity

The school will:

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

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.

Education

Online Safety Education Programme

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

The school delivers a Early years appropriate planned programme of online safety education, 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, is matched to need, and is taught through existing curriculum areas.

Staff

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

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include:
- A planned programme of online safety training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- 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 are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles
- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. [ProjectEVOLVE EDU](#)) and, where appropriate, enhanced pathways (e.g. [ProjectEVOLVE SAFEGUARDING](#)).
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

Governors

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

Training and updates may be provided through :

- Attendance at training offered by the Local Authority or other relevant organisations (e.g. SWGfL).
- Participation in information sessions.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

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

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

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

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

Working with Parents and Carers

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

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving 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.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions 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
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

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

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

Technology

Purpose

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

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](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The filtering and monitoring provision is provided by Lancashire County Council, Education Digital Services – Netsweeper. 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 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.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using [Testfiltering](#)). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record 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

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. (KCSIE 2026 refers to the [DfE Cyber Security Standards](#) and recognises cyber security as a safeguarding issue).

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 their safeguarding implications 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 [Data \(Use and Access\) Act 2025](#) makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

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
- 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.

Review

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

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

Technology Practice

Purpose

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

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

Detailed arrangements are set out in the relevant policy template appendices, including the Technical Security, Cyber Security, Data Security, Filtering and Monitoring, Device Management and Public Online Communications templates.

Device Management

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

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, 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
- learners 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 policies (in line with the [DfE statutory guidance](#))
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons
- 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.

Digital Content

The school 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.

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
- school-approved platforms and accounts are used where content includes personal or sensitive information

- staff and learners 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.

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. 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](#)

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. ([guidance is available from UKSIC](#))
- To reduce the risk of images, video, audio or other content featuring staff or learners being copied, manipulated or misused, including through AI technologies, the school only adds children's hands, the back of their heads and activities onto Social Media.
- Staff can add children's photos onto the Parent App Weduc.
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

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
- 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.

Mobile Technologies Policy

Mobile technology devices may be a school owned or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include;

- security risks in allowing connections to your school network,
- filtering of personal devices, breakages and insurance,
- access to devices for all learners,
- avoiding potential classroom distraction,
- network connection speeds,
- types of devices,
- charging facilities,
- total cost of ownership

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset.

Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies.

- The school allows:

School/devices

Personal devices

	School owned and allocated to a single user	School owned for use by multiple users	Authorised device	Learner owned	Staff owned	Parent owned	Other professional owned
Allowed in school	Yes	Yes	Yes	No	Yes	No	Yes
Full network access	Yes	Yes	Yes	No	No	No	No
Internet only				No	No	No	Yes
No network access				No	No	No	No

The school has provided technical solutions for the safe use of mobile technology for school devices -

- All school devices are controlled through the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- All school devices are subject to routine monitoring.
- Pro-active monitoring has been implemented to monitor activity.

- The school recommends that the classroom Ipads and devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on Ipads and laptops to aid security.

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Users are responsible for keeping their classroom device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Staff are responsible for charging their own classroom devices and for protecting and looking after classroom devices while in the school.
- School devices are provided to support learning.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll.
- Staff should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher and staff direction.

Staffs use of personal devices

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school.
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day.

- Personal mobile phones, smartwatches, and similar smart devices on site (phones, smartwatches, earbuds).
- Smartwatches are permitted to be worn by staff and visitors but must be switched off or placed in 'do not disturb' / silent mode.
- Staff and visitors are strictly prohibited from opening or answering messages, taking phone calls, or recording any media using smartwatches while on site.
- If any staff member or visitor wears smart glasses, they must be turned off at all times while on school premises.
- Devices must be in silent mode on the school site.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances such as entering into lockdown procedure and emergency services must be contacted if not able to contact the main office.
- Printing from personal devices will not be possible

How to raise a concern or get help

If something online worries you, we want to know.

- Learners: talk to a trusted adult, your tutor/class teacher, or the safeguarding team.
- Parents/carers: contact [DSL name / safeguarding email/phone].
- Staff: follow safeguarding procedures and record concerns promptly.

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

Links to other organisations and resources

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in August 2026. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2026

Pupil Acceptable Use Policy

We teach our Golden Rules which is as follows -

This is how we stay safe when we use computers:

- I will ask a grown-up before I use the tablet or computer.
- I will only use the internet when a grown-up is with me.
- I will be gentle with the tablet, keyboard and mouse.
- If I'm not sure, I will ask a grown-up for help.
- If I see something that makes me upset, I will tell a grown-up straight away.
- If I do not follow the rules, I may not be able to use the tablet.

Staff (and Volunteer) Acceptable Use Agreement Template

School Policy

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

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that filtering and monitoring are safeguarding measures designed to protect learners, staff and school systems. Where my role requires it, I will act promptly on concerns or alerts in accordance with the school's safeguarding procedures.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.

- I will immediately report any safeguarding, cyber security, filtering, monitoring or data protection concern using the school's agreed reporting procedures.
- I will complete the online safety, safeguarding and cyber security training required by the school and keep my knowledge up to date.

Protecting Learners, School Systems and Information:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will only communicate with learners, parents/carers and colleagues using school-approved systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
 - will only use AI technologies approved by the school
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
 - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
 - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
 - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance

- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- I recognise that AI supports, but does not replace, my professional judgement. I remain responsible for the accuracy, appropriateness and safeguarding implications of any AI-assisted work.
- I will follow the school's expectations for the professional use of mobile phones and other connected devices, ensuring only permitted use including -
 - **Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day.**
 - **Smartwatches are permitted to be worn by staff and visitors but must be switched off or placed in 'do not disturb' / silent mode.**
 - **Staff and visitors are strictly prohibited from opening or answering messages, taking phone calls, or recording any media using smartwatches while on site.**
 - **If any staff member or visitor wears smart glasses, they must be turned off at all times while on school premises.**
 - **Devices must be in silent mode on the school site.**
 - **Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances such as entering into lockdown procedure and emergency services must be contacted if not able to contact the main office.**
 - **Printing from personal devices will not be possible**

- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will protect school systems by following the school's cyber security procedures.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will respect filtering, monitoring and other security measures and report any concerns about their effectiveness.
- I understand that some websites or services may be restricted for safeguarding reasons and will use the school's agreed process where access is required for legitimate educational purposes.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal

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

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

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

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

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

- I understand that my professional responsibilities extend to my conduct in public online spaces where this could affect learners, colleagues or the reputation of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I will model safe, responsible and balanced use of digital technology in my professional practice.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

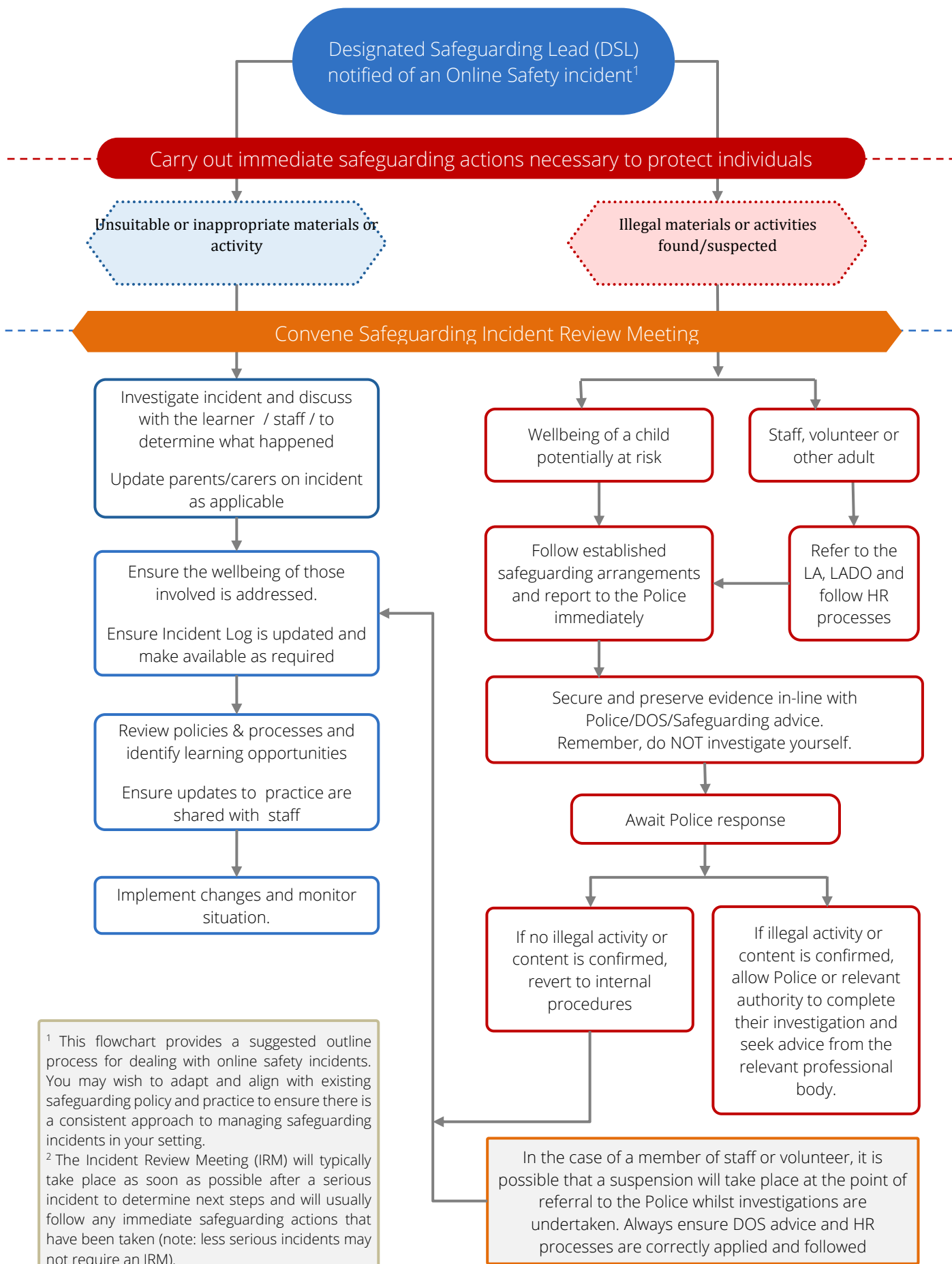
I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Responding to incidents of misuse – flow chart



Data Security Policy

Purpose

The purpose of this policy is to ensure that personal and sensitive data is handled securely, lawfully and transparently, in line with UK data protection legislation and statutory guidance. The policy supports safeguarding, privacy, and trust across the school community and forms part of the school's wider approach to online safety and information security.

Scope

This policy applies to:

- All personal data processed by the school
- All staff, volunteers, governors and contractors
- Data subjects including staff, learners and parents/carers
- All digital and paper-based records
- All third parties processing data on behalf of the school

Legislative Context

The school complies with current UK data protection legislation, including UK GDPR as amended and supplemented by applicable UK legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025, where relevant to the school's processing activities
- Freedom of Information Act
- Relevant guidance from [the Information Commissioner's Office](#) (ICO)

Policy Statement

The school recognises its role as a Data Controller and is committed to ensuring that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only for as long as necessary
- Secured against unauthorised access, loss or misuse

Data security is recognised as a safeguarding responsibility and is embedded across leadership, governance and daily practice.

AI-enabled or automated systems involving personal data are assessed before use, including consideration of lawful basis, transparency, data minimisation, security, accuracy, bias and the need for human oversight.

Personal or sensitive information will only be entered into approved AI systems where the school's data protection and security requirements have been satisfied.

Governance and Roles

Data Protection Officer (DPO)

The school will appoint a Data Protection Officer (internal or external) who:

- Provides independent advice and monitoring of compliance
- Supports Data Protection Impact Assessments (DPIAs)
- Acts as the point of contact with the ICO
- Reports directly to senior leadership and governors

The DPO operates independently and is supported with appropriate time, access and resources.

Governors

Governors:

- Approve and review data protection policies
- Provide strategic oversight of compliance and risk
- Ensure adequate resources are allocated
- Receive reports on data breaches, audits and risks

Senior Leaders and Staff

Senior leaders ensure that:

- Data protection is embedded into systems and culture
- Staff receive appropriate training
- Procedures are implemented consistently
- Data breaches are managed in line with school policy and in accordance with ICO guidance

All staff and governors are responsible for handling personal data securely and reporting concerns or incidents promptly.

Lawful Processing and Transparency

The school will:

- Identify and document lawful bases for processing personal data
- Apply additional conditions for processing special category data
- Maintain clear and accessible Privacy Notices for learners, parents/carers, staff and governors
- Ensure data subjects understand their rights
- Ensure consent is considered and established with data subjects and used only where appropriate and never as a default where a public task or legal obligation applies.

Records, Mapping and Risk Management

The school will maintain:

- A Record of Processing Activities (RoPA)
- A data asset register, including third-party and cloud services
- Clear retention and disposal schedules
- Data Protection Impact Assessments (DPIAs) for new or high-risk processing

Data protection is considered at the design stage of any new system or process (“data protection by design and default”).

New EdTech and cloud services are subject to appropriate data-protection, security and contractual checks before implementation.

Data Security and Access Controls

The school will ensure that:

- Access to personal data is role-based and restricted
- User accounts are protected by strong authentication
- Devices accessing personal data are secured and encrypted where appropriate
- Personal data is stored only on approved systems
- Cloud services meet UK data protection and security requirements
- Third-party contracts include appropriate data processing clauses
- Paper records are stored securely and disposed of appropriately.

Data Sharing and Transfer

Personal data will only be shared:

- Where there is a lawful basis
- With appropriate safeguards in place
- Using secure transfer methods
- With approved third parties

Additional care is taken when data is accessed remotely or transferred off-site.

Data Subject Rights

The school will uphold all data subject rights, including:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict or object to processing

Procedures are in place to manage requests within statutory timescales.

Data Breaches and Incident Management

The school will:

- Maintain clear procedures for reporting and managing data breaches
- Assess the risk to individuals' rights and freedoms
- Notify the ICO within 72 hours where required
- Record all breaches and near-misses
- Use learning from incidents to improve practice

Data breaches are treated as serious incidents and may also trigger safeguarding procedures where appropriate.

Training and Awareness

The school will ensure that:

- All staff and governors receive regular data protection training
- New staff receive training as part of induction
- Targeted training is provided where roles require it
- Learners are taught about privacy and data protection as part of the curriculum, in an age-appropriate way

Monitoring and Review

This policy will be:

- Reviewed at least annually
- Updated in response to changes in legislation, guidance or risk
- Supported by audits and compliance checks

Status

This Data Security Policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Technical Security Policy
- Cyber Security Policy
- Records Management and Retention Policy

Public Online Communications Policy

Purpose

The purpose of this policy is to set out how the school manages public online communications in order to reduce risk, promote safeguarding and online safety, celebrate success and communicate effectively with the wider school community.

Public online communications include the school website, newsletters, learning platforms, public messaging systems and official social media accounts.

This policy supports the Online Safety, Filtering and Monitoring, Technical Security, Cyber Security and Data Security policies and reflects [Keeping Children Safe in Education](#) (KCSIE), DfE digital and technology standards, UKSIC guidance [Best Practices for Managing Images and Videos on School Websites](#), DfE statutory publication requirements ([Maintained schools](#)) and ([Academies](#)).

Scope

This policy applies to:

- All staff and governors
- All public online communications representing the school
- Official school accounts and platforms
- Personal accounts where their use directly references, represents or could reasonably be associated with the school in a professional context
- School content published at any time, from any location or online platform

Policy Statement

The school will ensure that:

- Public online communications are accurate, lawful and appropriate
- Safeguarding considerations are prioritised
- Personal data is protected in line with the Data Security Policy
- Images and video are published only in line with consent procedures
- Copyright and intellectual property are respected
- Communications reflect professional standards
- Public references to the school are monitored appropriately
- Official public communications are made only through authorised school accounts and platforms.
- AI-generated or AI-assisted content is subject to appropriate human review and transparency labelling before publication.

Roles and Responsibilities

- Governors provide strategic oversight and assurance that public online communications meet safeguarding, data protection and statutory publication requirements.
- Senior leaders approve official accounts and oversee monitoring and moderation processes.
- Account administrators maintain secure access, monitor content regularly and ensure policy compliance.
- All staff must follow this policy, maintain professional standards and report concerns.

Creation of Public Online Accounts

- New public online accounts may only be created following approval by senior leadership.
- Proposals must define purpose, audience, responsible staff members and monitoring arrangements.
- Official accounts will be reviewed regularly and securely transferred, archived or closed when no longer required or when responsibility changes.

Monitoring and Moderation

The school will ensure that:

- Public communications are monitored regularly
- Comments are reviewed and moderated appropriately
- Harmful or inappropriate content is addressed appropriately, including removal, reporting, preservation of evidence or escalation where necessary.
- Safeguarding concerns are reported immediately through the school's safeguarding procedures; other serious incidents are recorded and escalated to senior leaders or relevant external agencies as appropriate.
- Harmful or inappropriate content is removed
- Serious incidents are recorded and escalated where necessary

Professional Standards

All public communications must:

- Be respectful and professional
- Avoid discriminatory, offensive or defamatory content
- Protect confidentiality
- Avoid internal grievance discussions
- Avoid disclosure of sensitive information

Use of Images and Media

The school will ensure that:

- Appropriate consent is obtained
- Images are appropriate and dignified
- Learners are not identified unnecessarily
- Images are removed where consent is withdrawn
- (n.b., UKSIC guidance [Best Practices for Managing Images and Videos on School Websites](#))
- Staff consider whether location and context published alongside images could increase safeguarding or privacy risks.

Personal Use and Association with the School

Staff may use personal social media accounts; however:

- Where staff identify themselves as associated with the school, they must maintain appropriate professional boundaries and comply with relevant staff conduct and acceptable use expectations.
- Personal use must not impact professional standards nor school reputation
- Staff must not engage with current learners via personal accounts
- Excessive or inappropriate use during working hours may result in disciplinary action

Handling Complaints and Abuse

Where negative comments are made online:

- The school will respond proportionately
- Abusive, threatening or harmful content will be managed proportionately, including recording, reporting, blocking, removal or referral to relevant platforms or agencies as appropriate.
- Abusive content should be challenged and removed
- Parents'/carers' complaints should be directed to formal complaints procedures
- Serious matters may be escalated to senior leaders or external agencies

Training and Awareness

The school will ensure that:

- Staff responsible for public accounts receive appropriate guidance and training on safeguarding, data protection, account security, moderation, escalation and the responsible use of AI-assisted content.
- Governors understand oversight responsibilities
- The wider community is informed of expected standards

Review and Continuous Improvement

This policy will be reviewed annually and updated in response to legislative changes, national guidance or emerging risks.

Legislation

This policy is informed by KCSIE, UK GDPR, Data Protection Act 2018 and the Online Safety Act 2023.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

[Harmful Sexual Support Service](#)

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

Kent – [Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Tools / Resources for Schools / other organisations

Whisper Anonymous Reporting Tool - <https://swgfl.org.uk/products/whisper/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

SWGfL Test filtering - <http://testfiltering.com/>

SWGfL 360 Groups – [online safety self review tool for organisations working with children](#)

SWGfL 360 Early Years – [online safety self review tool for early years organisations](#)

Childline – [Report / Remove](#)

SWGfL- [Assisted Monitoring](#)

SWGfL – [Resources for Education](#)

DfE [Using AI in education settings: support materials](#)

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

UKSIC - [Safety Features on Social Networks](#)

[Children's Commissioner, TES and Schillings – Young peoples' rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

SWGfL - [ProjectEvolveEdu](#)

[UKCCIS – Education for a connected world framework](#)

[Department for Education: Teaching Online Safety in Schools](#)

Teach Today – www.teachtoday.eu/

Data Protection

DfE – [Data Protection in schools toolkit](#)

ICO Guides for Organisations

[ICO Guidance on taking photos in schools](#)

Professional Standards/Staff Training

DfE – [Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

SWGfL – [Online Safety Training](#)

Infrastructure/Technical Support/Cyber-security

DfE – [Technical Standards for Schools and Colleges](#)

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

SWGfL- [Assisted Monitoring](#)

Secure Schools – [Cyber Security](#)

Working with parents and carers

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

Childnet – [Trust Me](#)

Research

[Ofcom – Childrens Media Habits](#)

Ofsted: [Review of sexual abuse in schools and colleges](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in August 2026. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2026