

Online Safety Policy 2026

Document Control	
Title	Online Safety Policy
Date	June 2026
Supersedes	Online Safety Policy June 2026
Amendments	This version of the policy has been completely rewritten and is now more focussed, with more accessible language and reduced in length. Elements that have been moved from the main body e.g. Filtering and Monitoring Policy, are now included in the appendices. Updated curriculum section to reflect the new computing curriculum.
Related Policies/Guidance	ICT policy Behaviour policy Parent Code of Conduct SEN Policy Equality /Inclusion Policy Pupil Privacy Policy Preventing radicalization and risk assessment policy Safeguarding Policy Whistleblowing Staff Code of Conduct Data Protection Policy Privacy Notices regarding use of data Mobile Phone Policy Searching and Confiscation Policy
Review	June 2027 – Or sooner if legislation is updated – e.g. KCSIE

Approved by: Trust Board

Date: 21.07.26

Last reviewed on: June 2026

Next review due by: June 2027

Contents

Scope of the Online Safety Policy	3
Rights Respecting Schools.....	4
Policy development, monitoring and review.....	4
Schedule for development, monitoring and review.....	5
Monitoring the impact of the policy.....	5
Policy and leadership	5
Why Online Safety Matters.....	5
Responsibilities	6
Online Safety Group	9
Policy.....	10
Online Safety Policy.....	10
Acceptable use.....	10
User actions.....	11
Communications	13
Reporting and responding	15
Responding to Pupil Actions.....	18
Responding to Staff Actions.....	19
Use of Artificial Intelligence (AI)	20
Online Safety Education Programme	22
Technology.....	25
Filtering & Monitoring.....	25
Technical Security.....	25
Cyber Security	26
Data Protection.....	26
Technology Practice.....	27
Device Management.....	27
Staff Personal Devices.....	28
Digital Content	28
Public Online Communications.....	29
Accessing learning from home.....	30
Remote Education.....	30
Digital Platforms	30
Safeguarding During Remote Education	30
Expectations for Staff	30
Expectations for Pupils	31
Cameras, Audio and Recording	31

Review	31
Outcomes.....	32
A1 – Online Safety Curriculum - PSHE and Computing.....	33
Computing and Online Safety	33
ProjectEVOLVE, PSHE and Education for a Connected World.....	34
PSHE, Relationships Education and Online Safety	34
A2 Pupil Acceptable Use Agreement Template – for KS2.....	37
A3 Learner Acceptable Use Agreement Template – for younger pupils (EYFS/KS1).....	39
A4 Parent/Carer Acceptable Use Agreement Template.....	40
A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template.....	42
A12 Reporting Log.....	47
B1 Training Needs Audit Log	48
B2 Staff request form template to change filtering or monitoring system	49
B3 Filtering and monitoring: checks template.....	50
C1 Filtering and Monitoring Policy.....	51
C2 Technical Security Policy	54
C3 - Cyber Security Policy	56
C6 – Public Online Communications Policy.....	58
Legislation	61
Links to other organisations or documents.....	67

Scope of the Online Safety Policy

This Online Safety Policy sets out how Newall Green 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.

The school recognises that online risks may arise through content, contact, conduct and commerce, as identified within Keeping Children Safe in Education and the Education for a Connected World Framework. This policy seeks to reduce risk across all four areas whilst enabling pupils to benefit safely from the opportunities that technology provides.

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, Newall Green 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.

Rights Respecting Schools

Newall Green Primary School is committed to the principles of the UNICEF Rights Respecting Schools Award. We recognise that children have rights both online and offline, and that online safety is an important part of protecting those rights. Through this policy, the school aims to ensure that all children can access technology safely, develop positive digital relationships and be protected from harm whilst online.

This policy particularly supports:



- **Article 19** – Children have the right to be protected from all forms of violence, abuse and neglect.
- **Article 17** – Children have the right to access information and material from a variety of sources, provided it is safe and appropriate.



• **Article 16** – Children have the right to privacy and protection of their personal information.



This policy has been developed in line with the school's Rights Respecting ethos and supports children to become safe, responsible and active digital citizens who understand both their rights and their responsibilities online.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *Online Safety Group* drawing on the expertise and responsibilities across the school. Membership includes:

- *headteacher/senior leaders*
- *Designated safeguarding lead (DSL)*
- *Online Safety Lead (OSL)*
- *staff – including teachers/support staff/technical staff*
- *governors*
- *parents and carers*

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 development, monitoring and review

This Online Safety Policy was approved by the <i>school Trustees</i> on:	7th July 2026
The implementation of this Online Safety Policy will be monitored by:	Online Safety Lead
Monitoring will take place at regular intervals:	<i>Yearly</i>
The <i>Trustees</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Termly</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>June 2027</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>MAT Trustees</i> <i>LADO</i>

Monitoring the impact of the policy

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

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

Policy and leadership

Why Online Safety Matters

Technology plays an important role in children's lives and offers significant educational, social and creative opportunities. Newall Green Primary School is committed to helping children benefit from these opportunities whilst developing the knowledge, skills and resilience needed to navigate online risks safely. Online safety is therefore viewed as a safeguarding priority and an essential part of preparing children for life in a digital world.

Responsibilities

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

Headteacher and senior leaders

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

Senior leaders will:

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

Governors and Trustees

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

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

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with DfE standards.
- Report to the relevant Trustee committee: **Audit, Risk and Finance**
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Participate in the Online Safety Group.
- Governors also support parent/carer and community engagement in online safety.

Designated Safety Lead (DSL)

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

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.

- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information, confirming at least annual checks.
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

An Online Safety Lead (OSL) may support delivery; the DSL retains lead responsibility.

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.

Curriculum Leads

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

Teaching and support staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture. The school promotes a culture of continuous improvement in digital competence, online safety and cyber security. Staff are encouraged to reflect on their practice, share learning and develop confidence in emerging technologies whilst maintaining appropriate safeguards.

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.
- Understand that their online presence and digital reputation can impact public confidence in the school and should therefore maintain professional standards in all online activity.
- Be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.

- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards.

Where services are outsourced, the school remains accountable.

The IT provider will:

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

Pupils

Pupils will:

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

Parents and carers

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

The school will:

- Publish the Online Safety Policy and share the learner AUA
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share online safety information through newsletters, parent information events, the school website, social media channels and national awareness campaigns such as Safer Internet Day.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. In some schools it may sit within a wider safeguarding or digital strategy group.

Membership

- DSL, OSL, Senior Leader(s)
- Online Safety Governor
- IT/technical representative (internal or provider)
- Staff representatives (teaching/support)
- The Online Safety Group may seek input from pupils and parents/carers through surveys, consultation activities and learner voice opportunities.

Core responsibilities

The group supports the DSL/OSL to:

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

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside 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, 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) ([see appendices](#)). AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

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

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	- Disabling, impairing or disrupting network/services (e.g., denial of service) - Using penetration-testing tools without explicit permission <i>Note: School will 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	

Communications

A wide range of rapidly developing communication technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies and clearly states what is allowed and not allowed.

Communication Technologies:	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming and in-game chat/voice (e.g. <i>Roblox, Fortnite, Minecraft</i>)			✓					✓
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)			✓		✓			
Cloud storage and file sharing (e.g., <i>Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents</i>)		✓			✓			
Social media and user-generated platforms (e.g. <i>TikTok, Instagram, Snapchat, X, Reddit</i>) and other age-restricted services			✓		✓			
Messaging, chat and voice (e.g., <i>WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts</i>)		✓			✓			
Streaming entertainment/media (video, music, podcasts) e.g. <i>Netflix, Disney+, Spotify</i>			✓		✓			
Video platforms and livestreaming (e.g. <i>YouTube, Twitch, TikTok LIVE, Instagram Live</i>)			✓		✓			
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds)			✓		✓			
Mobile phones used for learning (teacher-directed and supervised)		✓				✓		
Mobile phones used during social time/breaks (where permitted) including device-free approaches	✓				✓			
Taking photos/video/audio on devices (including sharing, location data and consent)		✓			✓			

Online gaming and in-game chat/voice (e.g. Roblox, Fortnite, Minecraft)	✓				✓			
Use of school devices		✓				✓		
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 *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

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

Reporting Concerns

The school will ensure that:

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

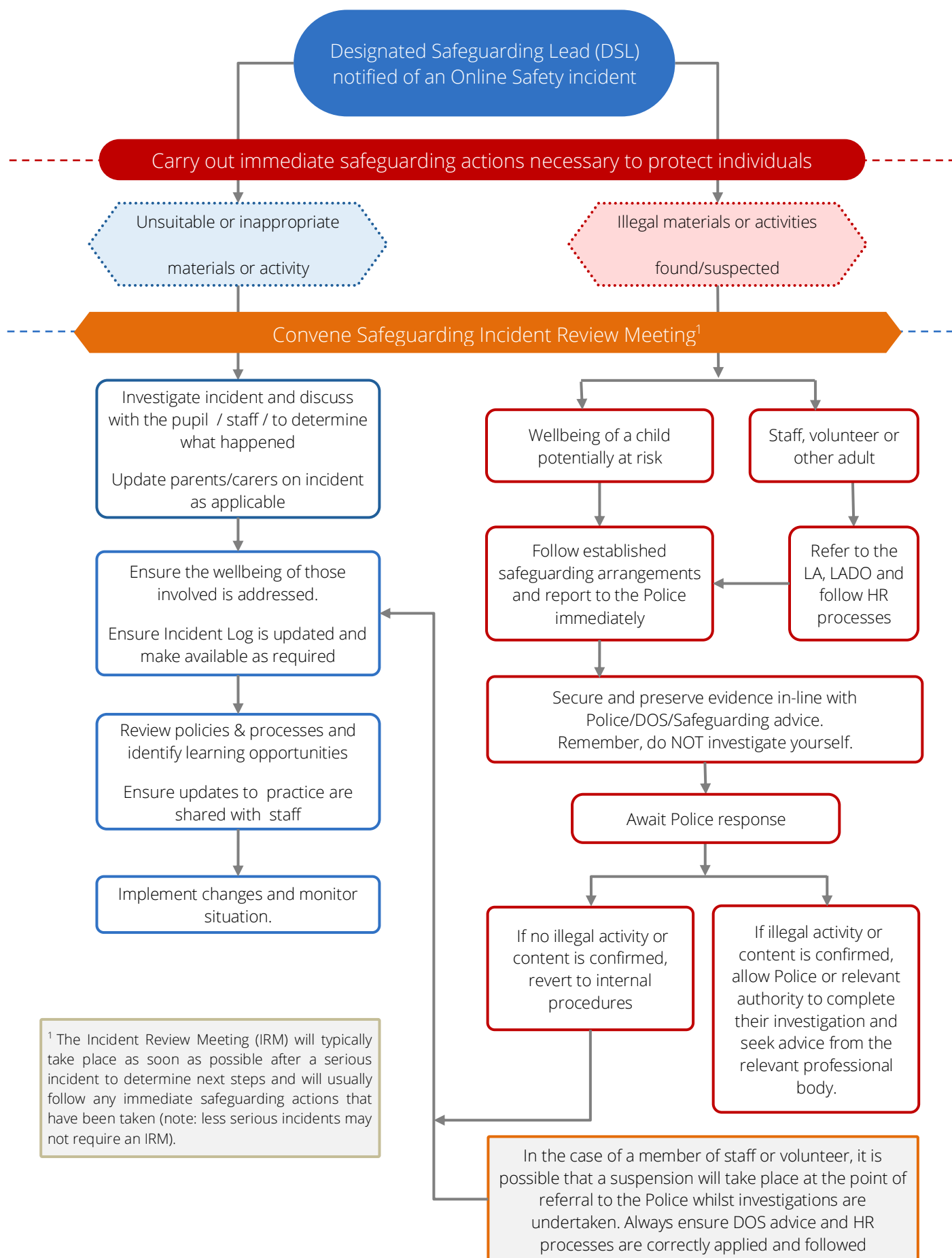
- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to: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

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)

The school will make the flowchart in appendix A10 - Responding to incidents of misuse – flow chart- available to staff to support the decision-making process for dealing with online safety incidents.



School actions

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

Responding to Pupil Actions

Incidents:	Refer to class teacher	Refer to DSL / OSL	Refer to Headteacher / SLT	Refer to Police/Social Services	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Accessing illegal material (or attempting to), as defined in the earlier “Unsuitable/Inappropriate Activities” section.		X	X	X					
Unauthorised access to the school network , including using another person’s account or sharing usernames/passwords.	X				X			X	
Unauthorised use of devices , including taking photos/videos or audio recordings.	X		X			X		X	
Unauthorised use of online services (apps, websites or platforms).	X					X		X	
Unauthorised downloading/uploading , file sharing or distribution of files.	X	X			X				
Damaging, corrupting or deleting another user’s data.					X				X
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).		X			X	X		X	
Failing to report accidental access to offensive or pornographic material		X	X	X	X	X		X	X
Deliberately accessing offensive or pornographic material (or attempting to)		X	X	X	X	X	X		X
Sharing or receiving content that breaches copyright or data protection law.			X						X
Sending offensive, harassing or bullying emails, texts or messages.		X	X	X		X	X		X
Any online behaviour that could bring the school into disrepute or undermines the school’s ethos.		X	X			X			X
Repeated breaches of these rules following previous warnings or sanctions.		X	X	X		X	X		X

Responding to Staff Actions

Incidents:	Refer to line manager	Refer to Headteacher / SLT	Refer to Local Authority / HR	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning / note of guidance	Further Disciplinary action in line with Disciplinary Policy and Code of Conduct
Accessing illegal material (or attempting to), as defined in the earlier “Unsuitable/Inappropriate Activities” section.		X	X	X			X
Breaching data protection or cyber-security requirements , including network security rules.	X	X			X	X	X
Accessing offensive or pornographic material (or attempting to).		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	X	
Unauthorised account/network access , including sharing passwords, using another person’s account, or allowing others access.	X				X	X	
Damaging systems or data , including corrupting/deleting others’ data or deliberately damaging hardware/software.		X			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			X
Inappropriate personal use of school technology , including personal email and social media use during work time/using school systems.	X	X				X	
Mishandling personal data , including storing, displaying or transferring it insecurely.	X					X	
Any action that undermines professional conduct or a staff member’s professional standing.		X	X				X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X				X
Failing to report incidents , whether accidental or deliberate.		X	X		X	X	
Repeated breaches following previous warnings or sanctions.		X	X				X

Use of Artificial Intelligence (AI)

For more detailed information on AI, please see our [Use of AI in School policy](#)

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.

We recognise that AI can be used to create or manipulate harmful content, including deepfakes and AI-generated intimate imagery. Such incidents will be treated as safeguarding concerns and managed in accordance with the school's safeguarding and child protection procedures.

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 Designated Safeguarding Lead, Online Safety Lead, Headteacher or Senior Leadership Team through the school's established reporting systems.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices in Appendix C7.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support 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.

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 planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including [DfE "Teaching Online Safety in Schools"](#), [UKCIS "Education for a Connected World"](#), and resources such as [SWGfL ProjectEVOLVE](#) and [Teach Computing](#).) Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education and Computing), with assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, unwanted contact, inappropriate online behaviour and online scams;
- understand personal boundaries, consent, respectful relationships and how to seek help if they experience worrying or inappropriate behaviour online;
- think critically about what they see online, including how to check whether information is reliable and recognise that some content may be generated by AI;
- understand that online content belongs to its creator and learn how to use information, images and AI tools responsibly;
- understand and follow the learner acceptable use agreement, behave responsibly online and recognise that their online actions have consequences.

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Where learning activities require access to additional online resources, staff will ensure appropriate supervision and safeguards are in place.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities.

Staff

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

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include: understanding harmful content, understanding harmful behaviours, use of technology and risk, the dark web, cyber security and policy, roles and responsibilities.

- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. [SSS](#)) and, where appropriate, enhanced pathways (e.g. [ProjectEVOLVE SAFEGUARDING](#)) or [The Key](#)).
- 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/Trustees

Governors/Trustees 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 (select/delete as appropriate):

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

Enhanced training will be provided for (at least) the Online Safety/Safeguarding 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, and that many external bodies can enhance the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

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

Working with Parents and Carers

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

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carers 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.

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

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 & 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 including Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring Standards.

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 personal devices are permitted to access school systems, users understand that activity may be subject to filtering and monitoring.

Oversight and Review

The school recognises that filtering and monitoring are important safeguarding measures but do not replace effective supervision, education, reporting procedures or professional judgement.

Senior leaders, the Designated Safeguarding Lead, technical staff and governors have clearly defined responsibilities for filtering and monitoring. The effectiveness of filtering and monitoring arrangements is reviewed at least annually, and following significant incidents, safeguarding concerns or changes to technology.

The school uses recognised tools and guidance, including Senso, Senso Browser and SWGfL Test Filtering, to evaluate the effectiveness of its filtering provision.

Further detail regarding filtering and monitoring systems, responsibilities, review procedures and operational arrangements is provided in **Appendix C1 – Filtering and Monitoring Arrangements**.

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.

Further detail is provided in the **Appendix C2 - Technical Security Procedures**.

Cyber Security

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

The school ensures that:

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

Further detail is provided in the **Appendix C3 – Cyber Security Policy**

Data Protection

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

The school ensures that:

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

Further detail is provided in our Data Protection Policy.

Review

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

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

Technology Practice

Purpose

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

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

Detailed arrangements are set out in the Appendix C2 - Technical Security Procedures and Appendix C6 – Public Online Communications

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

Staff Personal Devices

Staff may bring personal mobile phones and smart devices onto the school site. Devices must be used in accordance with the Staff Acceptable Use Agreement, Staff Code of Conduct and Online Safety Policy.

Staff must not:

- Use personal devices to photograph, video or record pupils.
- Use personal devices to communicate with pupils.
- Use personal devices to communicate with parents outside approved school systems.
- Store school data on personal devices.
- Use unapproved AI tools for school business.

Personal devices should be stored securely and used only during break times, Multi-Factor Authentication (MFA), emergencies, medical needs or where authorised by senior leaders.

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	Yes – with permission	No
Internet only	Yes	Yes	Yes	No	Yes – with permission	Yes
No network access	Yes	Yes	Yes	Yes	Yes	Yes

Digital Content

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

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

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

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. ([guidance is available from UKSIC](#))
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour

Review

Technology practice is reviewed regularly to reflect:

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

Accessing learning from home

Remote Education

Newall Green Primary School recognises that there may be exceptional circumstances where pupils are unable to attend school but remain well enough to access learning remotely. Where appropriate, the school will provide remote education in line with Department for Education guidance and individual pupil needs.

Remote education is intended to support continuity of learning and is not a replacement for regular school attendance. Decisions regarding remote education will be made on a case-by-case basis by school leaders.

Digital Platforms

The school uses Microsoft Teams and other approved educational platforms to support remote learning when required.

All school-approved platforms:

- Use secure, school-managed accounts.
- Comply with safeguarding and data protection requirements.
- Are subject to the school's filtering and monitoring arrangements where applicable.
- Are only used for educational purposes.

Pupils and families will be provided with login details and support where required.

Safeguarding During Remote Education

Safeguarding remains the school's highest priority whether learning takes place on-site or remotely.

The school will:

- Maintain appropriate professional boundaries at all times.
- Ensure staff use only school-approved communication systems.
- Record and report any safeguarding concerns in line with the Child Protection and Safeguarding Policy.
- Follow the Staff Code of Conduct and Acceptable Use Agreements.
- Take reasonable steps to ensure online learning environments remain safe and appropriate.

Any concerns identified during remote learning sessions will be reported immediately to the Designated Safeguarding Lead (DSL).

Expectations for Staff

When delivering remote education, staff will:

- Use only school-approved accounts and platforms.
- Maintain professional standards and conduct at all times.

- Ensure learning materials are appropriate, accessible and inclusive.
- Protect personal and confidential information.
- Follow safeguarding, online safety and data protection procedures.
- Report any concerns, incidents or breaches immediately.
- Ensure any AI tools used comply with the school's AI and data protection requirements.

Staff must not use personal social media accounts, personal messaging services or personal email accounts to communicate with pupils.

Expectations for Pupils

When accessing remote learning, pupils are expected to:

- Follow the Pupil Acceptable Use Agreement.
- Use school systems responsibly and respectfully.
- Treat staff and other pupils with courtesy and respect.
- Report any concerns, inappropriate content or worrying behaviour to a trusted adult.
- Keep usernames and passwords secure.
- Access only the learning activities provided by school staff.

The school's Behaviour Policy may be applied where inappropriate online behaviour affects members of the school community.

Cameras, Audio and Recording

The school recognises that video conferencing can support effective teaching and learning. Where live sessions are used:

- Participation is subject to parental agreement where appropriate.
- Staff will use school-approved accounts and platforms.
- Sessions will be conducted in a professional manner.
- Pupils should participate from an appropriate location wherever possible.
- Appropriate clothing and behaviour are expected from all participants.

Recording, photographing, screenshotting, livestreaming or sharing any part of an online lesson, meeting or communication without the explicit permission of the school is prohibited.

Any unauthorised recording or sharing of remote learning content may be treated as a safeguarding concern and managed in accordance with the school's Behaviour, Safeguarding and Online Safety Policies.

Review

The school's remote education arrangements will be reviewed periodically to ensure they remain effective, secure and aligned with current guidance and school practice.

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

Appendix

A1 – Online Safety Curriculum - PSHE and Computing
A2 - Pupil Acceptable Use Agreement Template – KS2
A3 - Pupil Acceptable Use Agreement Template – for younger pupils (Foundation/KS1)
A4 - Parent/Carer Acceptable Use Agreement Template
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A7 – Online Safety Group Terms of Reference Template
A10 - Responding to incidents of misuse – flow chart
A11 - Record of reviewing devices/internet sites (responding to incidents of misuse)
A12 - Reporting Log
B1 - Training Needs Audit Log
B2 - Staff request form template to change filtering or monitoring system
B3 - Filtering and monitoring: checks template
C1 – Filtering and Monitoring Policy Template
C2 - Technical Security Policy Template (including Technical Security and Device Management
C3 - Cyber Security Policy Template
C6 – Public Online Communications Policy Template
Legislation
Links to other organisations and resources

A1 – Online Safety Curriculum - PSHE and Computing

Computing and Online Safety

At Newall Green Primary School, online safety is taught through a combination of the National Centre for Computing Education (NCCE) Teach Computing Curriculum and ProjectEVOLVE, which is based on the UK Council for Internet Safety's Education for a Connected World Framework.

Online safety education is embedded throughout the computing curriculum and reinforced through PSHE, assemblies, themed events, safeguarding work and day-to-day use of technology. This ensures that pupils develop the knowledge, skills and behaviours required to use technology safely, respectfully, responsibly and securely.

Early Years Foundation Stage

Children begin to develop an understanding of technology and how it is used in everyday life. They learn to:

- Recognise technology used in school and at home.
- Understand that some information is private and should not be shared.
- Identify trusted adults who can help them if something online worries or upsets them.
- Understand the importance of being kind and respectful to others.
- Begin to understand healthy screen use and balancing online and offline activities.

Key Stage 1

Through Teach Computing units such as *Technology Around Us*, *Information Technology Around Us*, *Digital Writing*, *Digital Photography* and *Programming*, pupils learn to:

- Use technology safely and respectfully.
- Keep personal information private.
- Recognise trusted adults who can help if they encounter something worrying online.
- Understand that technology can be used to communicate and create content.
- Use digital devices responsibly within school.
- Recognise appropriate and inappropriate online behaviour.
- Develop an understanding of how technology affects their lives and the lives of others.
- Begin to understand how information can be shared online and the importance of making safe choices.

Lower Key Stage 2

Through Teach Computing units such as *Connecting Computers*, *The Internet*, *Branching Databases*, *Data Logging* and digital media projects, pupils learn to:

- Understand how computer networks and the internet enable communication and information sharing.
- Recognise that information found online may not always be accurate or trustworthy.
- Develop strategies for evaluating websites and online content.
- Create and share digital content responsibly.
- Understand the importance of secure passwords.
- Recognise age restrictions and why they exist.
- Understand digital footprints and the impact of online actions.

- Know how and where to report concerns about online content, contact or conduct.

Upper Key Stage 2

Through Teach Computing units such as *Systems and Searching*, *Communication and Collaboration*, *Web Page Creation*, *Video Production* and *Physical Computing*, pupils learn to:

- Understand how online information is searched, ranked and presented.
- Evaluate the reliability and validity of online sources.
- Understand copyright, ownership and plagiarism.
- Collaborate safely using digital technologies.
- Manage passwords and personal information securely.
- Recognise the risks associated with sharing information online.
- Understand how online activity contributes to a permanent digital footprint.
- Recognise how technology can influence wellbeing, relationships and reputation.
- Understand the benefits and risks of emerging technologies and online services.
- Demonstrate responsible, respectful and safe online behaviour.

ProjectEVOLVE, PSHE and Education for a Connected World

ProjectEVOLVE is used to supplement our Computing and PSHE curriculum, through a progressive online safety curriculum from EYFS to Year 6. Learning is organised around the eight strands of the Education for a Connected World Framework:

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Wellbeing and Lifestyle
- Privacy and Security
- Copyright and Ownership

These themes are revisited throughout a pupil's time at school, enabling children to build upon previous learning and develop age-appropriate knowledge, skills and behaviours for life in an increasingly digital world.

Online safety education is further supported through assemblies, safeguarding lessons, national awareness events, pastoral interventions and responsive teaching where emerging risks or concerns are identified.

PSHE, Relationships Education and Online Safety

Online safety is further developed through our PSHE curriculum, delivered through the Dimensions and Manchester Healthy Schools iMatter programmes. Through PSHE, pupils explore the social, emotional, health and relationship aspects of living in an increasingly digital world, enabling them to develop the skills, knowledge and resilience needed to stay safe online and offline.

Early Years Foundation Stage

Children begin to develop the foundations of safe and responsible behaviour by learning to:

- Identify trusted adults who can help them when they are worried or upset.
- Understand that some information is private and should not be shared.
- Develop positive friendships and respectful relationships.
- Recognise and talk about their feelings and emotions.
- Begin to understand how to stay safe when using technology at home and at school.
- Develop healthy habits and balance screen-based activities with play, physical activity and social interaction.

Key Stage 1

Through Relationships Education, Health Education and PSHE lessons, pupils learn to:

- Understand basic rules for staying safe online.
- Recognise what personal information is and why it should be kept private.
- Know how to seek help from a trusted adult if something online worries or upsets them.
- Understand that not everything seen online is true.
- Recognise that people may behave differently online than they do face-to-face.
- Develop an understanding of online kindness and respectful behaviour.
- Begin to recognise cyberbullying and understand how to report concerns.
- Understand how digital technology is used in everyday life and communication.
- Learn the importance of balancing screen time with healthy lifestyles and relationships.

Lower Key Stage 2

Through PSHE and Relationships Education, pupils learn to:

- Understand the importance of protecting personal information and privacy online.
- Recognise risks associated with sharing information, images and content online.
- Understand how information and data can be shared and used online.
- Develop strategies for responding to unwanted contact or inappropriate content.
- Recognise the importance of respectful online relationships and communication.
- Understand the emotional impact of online behaviour, including cyberbullying.
- Learn how to report concerns and access support when needed.
- Begin to critically evaluate online information and recognise misleading content.
- Understand age restrictions and why they exist to protect children.

Upper Key Stage 2

Through PSHE, Relationships Education and Health Education, pupils learn to:

- Understand the similarities and differences between online and offline relationships.
- Recognise the risks associated with communicating with people they do not know offline.
- Evaluate online information and understand how content can be ranked, targeted and influenced.
- Understand how online behaviour contributes to their digital reputation and digital footprint.
- Recognise the impact that social media, gaming and online activity can have on mental health and wellbeing.
- Develop strategies to manage screen time and maintain a healthy balance between online and offline activities.
- Recognise harmful online behaviours including cyberbullying, harassment, trolling and manipulation.

- Understand how to stay safe when sharing information, images and opinions online.
- Identify unhealthy or unsafe online relationships and know how to seek support.
- Demonstrate responsible, respectful and safe online behaviour as digital citizens.

Online Safety Through PSHE

Online safety learning within PSHE complements the Teach Computing curriculum by focusing on pupils' wellbeing, relationships, decision-making and personal safety. Together, the PSHE and Computing curricula ensure that pupils develop both the technical understanding and the personal resilience required to navigate the online world safely, responsibly and confidently.

A2 Pupil Acceptable Use Agreement Template – for KS2

Introduction

Using computers and other digital devices has become a part of everyday life for children and young people, both at school and outside of it. These devices are powerful tools that can help us learn, be creative, and understand the world around us. It's important for us to be able to use these devices safely.

Acceptable Use Agreement

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

Keeping Safe Online

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

Using Computers and the Internet Sensibly

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

Being Respectful and Responsible

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

What Happens If I Break These Rules?

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

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

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

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

Name of Learner:Group/Class:.....

Signed:Date:

Parent/Carer Countersignature

Name of Parent:

Signed:Date:

A3 Learner Acceptable Use Agreement Template – for younger pupils (EYFS/KS1)

Our Technology Rules

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

Staying Safe

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

Using Technology Kindly

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

Making Good Choices

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

What Happens If I Forget the Rules

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

Signed (child):.....

Signed (parent):.....

Date:.....

A4 Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications 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 parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name:

Learner Name:

As the parent/carers of the above pupils, I give permission for my son/daughter to have access to the digital technologies at school.

Either: (KS2)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (EYFS and KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed:

Date:

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parents'/carers' permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to sign the permission form to allow the school to take and use images of their children and for the parents/carers to agree.

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

A5 Staff (and Volunteer) Acceptable Use Policy 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 users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

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

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal 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 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
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.

- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

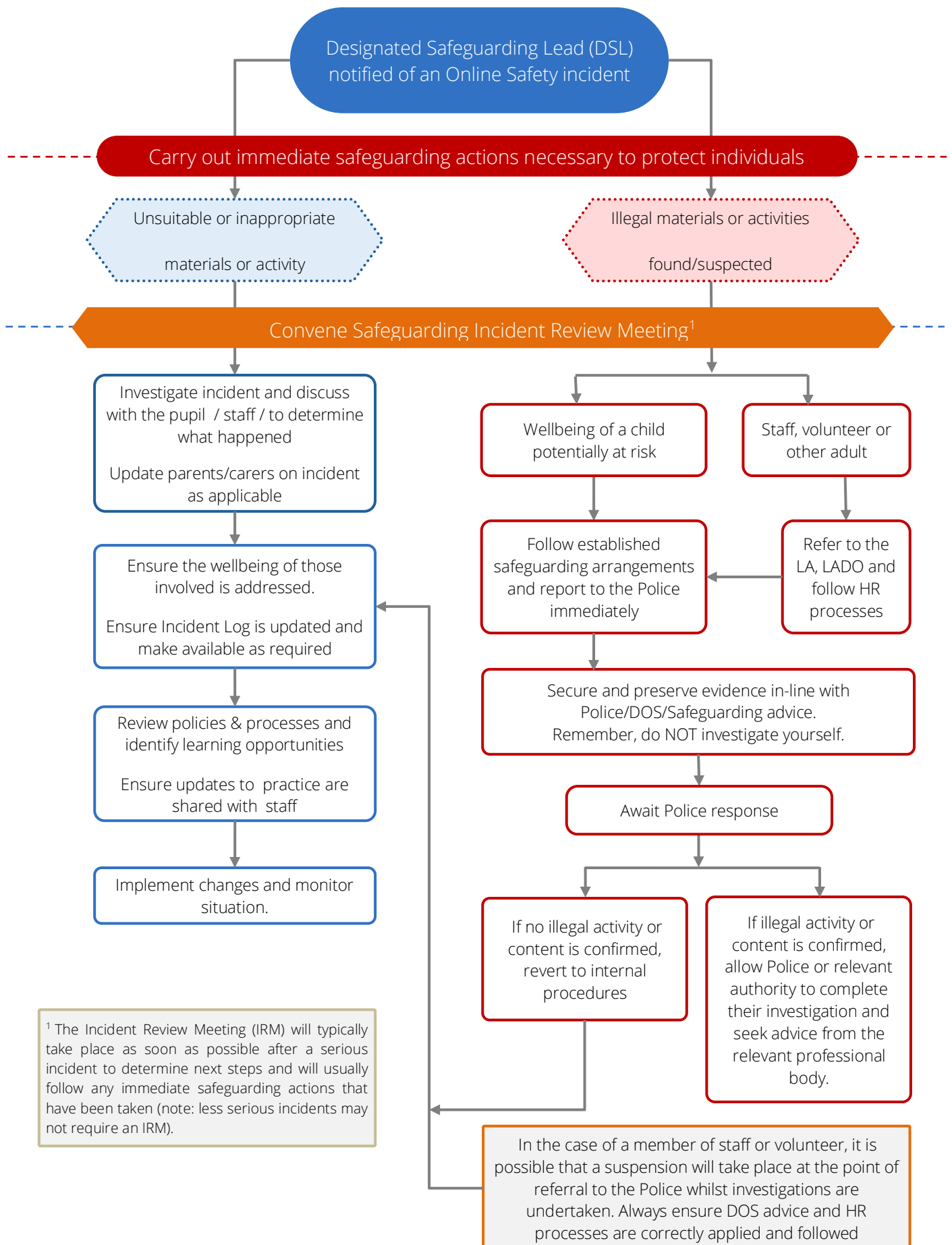
I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

A10 Responding to incidents of misuse – flow chart



A11 Record of reviewing devices/internet sites (responding to incidents of misuse)

Alternatively, record the below information on CPOMs or complete the form and add to CPOMs when linked to a pupil or staff member

Group:
 Date:
 Reason for investigation:

Details of first reviewing person

Name:
 Position:
 Signature:

Details of second reviewing person

Name:
 Position:
 Signature:

Name and location of computer used for review (for web sites)

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A12 Reporting Log

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

B1 Training Needs Audit Log

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

B2 Staff request form template to change filtering or monitoring system

Staff Name:

Year group

Website title and URL/link:

E.g. <https://www.youtube.com/>

Year group/user you want the website unblocked or blocked for (if applicable):

Year group/user:

Reason why you want the website unblocked/blocked:

E.g. students need to access it for classwork, homework, revision, inappropriate material, proxy website

Can we re-block/unblock this site after a specific date?

No ☐

Yes ☐

Date the website can be re-blocked/unblocked: _____

Agreed by (OSL/IT Provider):

Date agreed:

Date completed:

B3 Filtering and monitoring: checks template

CHECKS	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose? You can signpost your IT service provider to South West Grid for Learning's (SWGfL) testing tool.			
Is the system running and working?			
Have we checked that our filtering and monitoring system works on: All devices New devices and services before they're given to staff or pupils			
Have we reviewed the list of blocked sites on our network? Is this list still accurate/does it reflect any changes to safeguarding risks?			
Does our filtering system adhere to the requirements? (Get your checklist of the requirements here)			
Does our monitoring system adhere to the requirements? (Get your checklist of the requirements here)			

C1 Filtering and Monitoring Policy

Purpose

The purpose of this policy is to ensure that appropriate filtering and monitoring systems are in place to safeguard learners and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. Filtering and monitoring form part of the school's wider safeguarding responsibilities and are implemented in line with [Keeping Children Safe in Education](#) (KCSIE) and the [DfE Filtering and Monitoring and Technical Standards](#).

Scope

This policy applies to:

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

Roles and Responsibilities

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

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Pauline ??? – Safeguarding Governor
Senior Leadership/Online Safety Lead	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of our provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Alec Killingbeck – Deputy Headteacher (OSL)/Deputy Safeguarding Lead Adam Pattenden – Deputy Headteacher (Deputy OSL)/Deputy Safeguarding Lead

Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Sarah Rudd – Executive Headteacher/DSL Tom Rudd – Assistant Headteacher/DSL
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	HG-IT
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Policy Statement

The school will ensure that:

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

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

Filtering

The school will ensure that filtering systems:

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

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

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

The school will use recognised tools and guidance to assure the effectiveness of filtering provision e.g., [testfiltering.com](https://www.testfiltering.com)

Monitoring

The school will ensure that monitoring:

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

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

C2 Technical Security Policy

(including Access, Device and Incident Management)

Purpose

This policy sets out how the school protects its technical infrastructure, systems and devices to ensure a secure and resilient digital environment. It supports safeguarding, data protection and business continuity and aligns with the [DfE Technical Standards](#)

Scope

This policy applies to:

- Staff, learners and governors
- Suppliers of third-party services and solutions
- School networks, servers and cloud systems
- School-owned devices
- User accounts and access controls
- Device configuration and management, including personal devices where permitted

Policy Statement

The school will ensure that its technical systems are managed in a way that:

- Protects users and data from unauthorised access or misuse
- Supports safe and reliable access to digital services
- Enables detection, response and recovery from technical incidents
- Is proportionate to risk and regularly reviewed

Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights
- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect [NCSC](#) and [DfE guidance](#)
- Multi-factor authentication is used for sensitive systems where appropriate
- Administrator access is restricted and monitored
- System administrators and those with global/ confidential data system access use a physical security device in addition to MFA to access systems.

System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly
- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly, stored securely (both locally and offsite, with rotation) and regularly tested

- Physical access to infrastructure is controlled

Device Management

The school will ensure that:

- Clear expectations exist for the use of school-owned and personal devices
- School devices are configured securely and managed appropriately, with regular/automatic patches and updates
- Where personal devices are permitted, expectations are clearly defined and risk-assessed
- Acceptable Use Agreements reference responsible device use
- Users receive guidance on safe and appropriate device use

Supplier Management

The school will ensure that:

- Provision of third-party services and solutions are adequately contracted and regularly reviewed
- Suppliers can demonstrate adherence to school policy and alignment with the [DfE Technical Standards](#)

Incident Management

Technical incidents will be logged, escalated and reviewed. Serious incidents will be managed in line with safeguarding and business continuity procedures.

Review and Training

Technical security arrangements will be reviewed regularly. Staff with specific responsibilities will receive appropriate training, and users will be educated on their responsibilities.

C3 - Cyber Security Policy

Purpose

This policy sets out how the school prevents, detects, responds to and recovers from cyber threats. It supports the school's duty of care to protect users and data and aligns with the [DfE Cyber Security Standards](#), [National Cyber Security Centre \(NCSC\) guidance](#) and [NCSC Cyber Essentials](#)

Scope

This policy applies to:

- Cyber threats including phishing, ransomware, malware and unauthorised access
- Staff, learners and governors
- Suppliers of third-party services and solutions
- Technical systems and cloud services
- Incident response and business continuity

Policy Statement

The school will take a proactive, risk-based approach to cyber security to:

- Reduce the likelihood and impact of cyber incidents
- Ensure timely and effective response to threats
- Build awareness and resilience across the school community

Cyber Security Strategy

The school will maintain a cyber security strategy that:

- Is supported by senior leaders and governors
- Is informed by risk assessment and incident learning
- Is reviewed regularly in line with emerging threats
- Is inclusive of all services and solutions, including those from third-party suppliers

Supplier Management

The school will ensure that suppliers:

- Can demonstrate adherence to school policy and alignment with the [DfE Cyber Security Standards](#)
- Are familiar with school incident response plan and able to respond effectively

Awareness and Education

The school will ensure that:

- Staff receive regular cyber awareness training
- Learners receive age-appropriate education on cyber risks
- Governors understand their oversight responsibilities

Incident Response

The school will maintain a clear cyber incident response plan that:

- Defines roles and escalation routes
- Supported by an effective communications strategy
- Supports safeguarding and business continuity
- Is tested periodically through simulations or exercises
- Ensures incidents are recorded and reviewed

External Assurance

Where appropriate, the school will engage external expertise to assess cyber resilience and will work towards recognised standards or certifications.

Review

Cyber security arrangements will be reviewed annually, or sooner if required by incidents, guidance or changes in technology. Lessons learned from managing incidents should inform improvements to the strategy.

C6 – 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), 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 they directly reference or represent the school
- 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

Roles and Responsibilities

- Governors provide strategic oversight and ensure compliance with 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.
- At least two authorised staff members must have access to any official public account.

Monitoring and Moderation

The school will ensure that:

- Public communications are monitored regularly
- Comments are reviewed and moderated appropriately
- 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
- 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. (n.b., UKSIC guidance [Best Practices for Managing Images and Videos on School Websites](#))

Personal Use and Association with the School

Staff may use personal social media accounts; however:

- Where referencing the school, appropriate disclaimers must be used
- Personal use must not impact professional standards nor school reputation
- Staff must not engage with current pupils 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 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 guidance and training
- 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

Schools should be aware of the legislative framework under which this online safety policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the event of an online safety issue or situation.

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](#)

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.

- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;

- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly

- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carers to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

Online Safety Act 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Ofcom is the independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

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](#)